

**From:** [Sanderson, Mark](#)  
**To:** [Bartlett, Kelly](#); [Ruecroft, Daniel](#)  
**Cc:** [Bayliss, Michael](#); [Hollis, Jeremy](#)  
**Subject:** RE: Google - Spam pornographic  
**Date:** Friday, 14 August 2020 2:02:49 PM  
**Attachments:** [image002.jpg](#)  
[image003.jpg](#)  
[image004.jpg](#)  
[image005.png](#)

OFFICIAL

Hi Kelly  
We are investigating.  
Regards

**Mark Sanderson | Senior Director, Education ICT**

Phone: +61 2 6207 5191 | 0408 769 727

**Shared Services ICT | Chief Minister, Treasury and Economic Development Directorate | ACT Government**

Level 2 Winyu House 125 Gungahlin Place, Gungahlin | HBCTL Fremantle Dr Stirling | GPO Box 158 Canberra ACT 2601 |

[www.act.gov.au](http://www.act.gov.au)

*Please consider the environment before printing this email. If printing is necessary, print double-sided and black and white*



**From:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
**Sent:** Friday, 14 August 2020 1:55 PM  
**To:** Ruecroft, Daniel <Daniel.Ruecroft@act.gov.au>; Sanderson, Mark <Mark.Sanderson@act.gov.au>  
**Cc:** Bayliss, Michael <Michael.Bayliss@act.gov.au>; Hollis, Jeremy <Jeremy.Hollis@act.gov.au>  
**Subject:** RE: Google - Spam pornographic

OFFICIAL

Hi Guys  
We are receiving reports that access and emails are still occurring. Do we have any other options?  
Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)



**From:** Ruecroft, Daniel <Daniel.Ruecroft@act.gov.au>  
**Sent:** Friday, 14 August 2020 1:50 PM  
**To:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>; Sanderson, Mark <Mark.Sanderson@act.gov.au>  
**Cc:** Bayliss, Michael <Michael.Bayliss@act.gov.au>; Hollis, Jeremy <Jeremy.Hollis@act.gov.au>  
**Subject:** RE: Google - Spam pornographic

OFFICIAL

Hi Kelly and Mark,  
Quick update:  
Gmail blocked at CK for all students (blocking mail.google.com and gmail.com)

Gmail disabled for all students (Google report this can take up to [redacted] hours - see [How changes propagate to Google services.](#))

SSO Auth to google denied

Kind regards,

Daniel

---

**From:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>  
**Sent:** Friday, 14 August 2020 1:05 PM  
**To:** Rucroft, Daniel <[Daniel.Rucroft@act.gov.au](mailto:Daniel.Rucroft@act.gov.au)>  
**Cc:** Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; Hollis, Jeremy <[Jeremy.Hollis@act.gov.au](mailto:Jeremy.Hollis@act.gov.au)>  
**Subject:** RE: Google - Spam pornographic

OFFICIAL

approved

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)

---

**From:** Rucroft, Daniel <[Daniel.Rucroft@act.gov.au](mailto:Daniel.Rucroft@act.gov.au)>  
**Sent:** Friday, 14 August 2020 1:05 PM  
**To:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>  
**Cc:** Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; Hollis, Jeremy <[Jeremy.Hollis@act.gov.au](mailto:Jeremy.Hollis@act.gov.au)>  
**Subject:** RE: Google - Spam pornographic

OFFICIAL

Hi Kelly,

Seeking your approval to block gmail on content keeper for all students. Also seeking approval to temporarily disable the gmail service for students.

Kind regards,

**Daniel Rucroft | Director ICT Operations | Education Directorate**

**Customer Engagement Services Branch** | Shared Services ICT

Phone: +61 2 620 58473 | Email: [Daniel.Rucroft@act.gov.au](mailto:Daniel.Rucroft@act.gov.au)

**Shared Services** | Chief Minister, Treasury and Economic Development Directorate | **ACT Government**

Level 2, Winyu House 125 Gungahlin Place, Gungahlin ACT 2912 | GPO Box 158 Canberra ACT 2601 | [www.act.gov.au](http://www.act.gov.au)

---

**From:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>  
**Sent:** Friday, 14 August 2020 12:42 PM  
**To:** Rucroft, Daniel <[Daniel.Rucroft@act.gov.au](mailto:Daniel.Rucroft@act.gov.au)>  
**Subject:** Google - Spam pornographic  
**Importance:** High

OFFICIAL

Hi Daniel

Please disconnect all Google email traffic, until we are able to stop the spam.

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)

**From:** Williamson, Bill <Bill.Williamson@ed.act.edu.au>  
**Sent:** Friday, 14 August 2020 5:58 PM  
**To:** Sanderson, Mark <Mark.Sanderson@act.gov.au>; Ruecroft, Daniel <Daniel.Ruecroft@act.gov.au>; Bayliss, Michael <Michael.Bayliss@act.gov.au>  
**Cc:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
**Subject:** FW: ACT Education - Settings Changed

**Bill Williamson | Senior Director - School Administration System Architecture**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

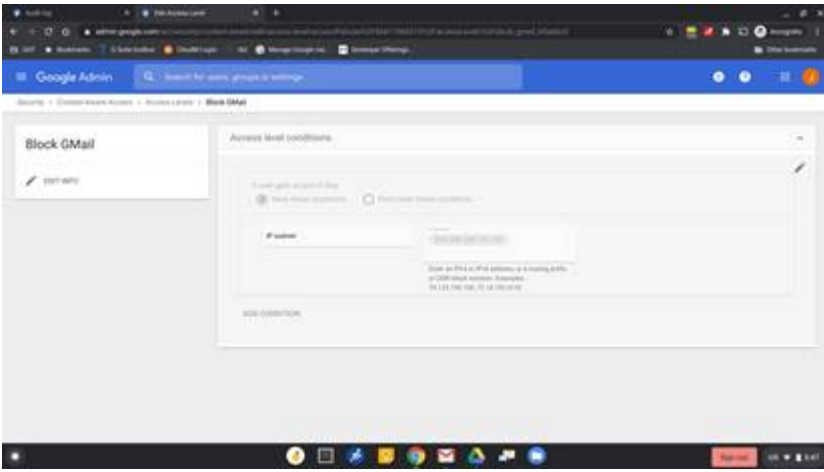
[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

**From:** [REDACTED] <[\[REDACTED\]@geeksontap.com.au](mailto:[REDACTED]@geeksontap.com.au)>  
**Sent:** Friday, 14 August 2020 5:56 PM  
**To:** Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>  
**Subject:** ACT Education - Settings Changed

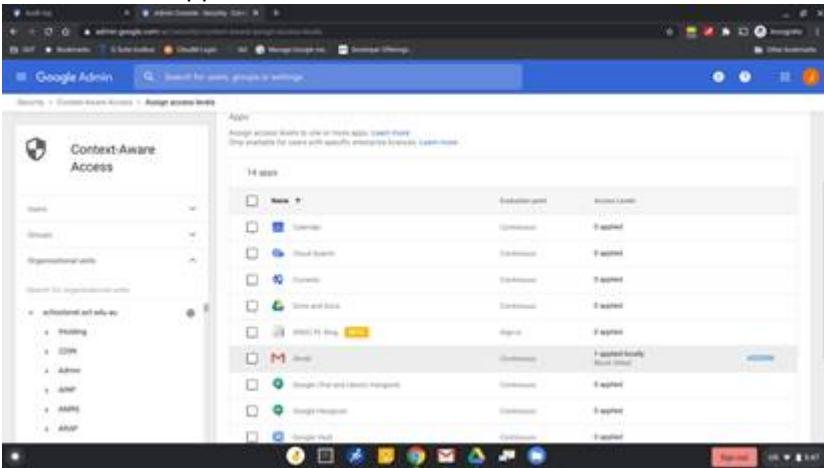
Hi Bill,

As discussed here are items that i changed.

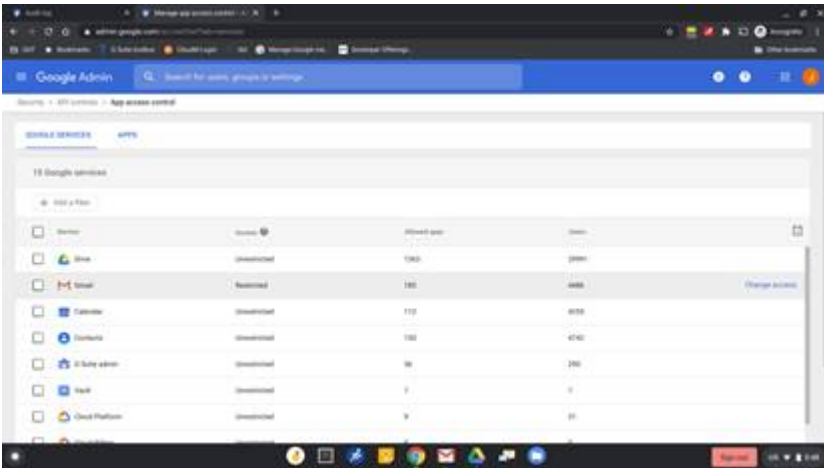
Enabled Context aware access to block access to GMail from everyone except from the IP address listed.



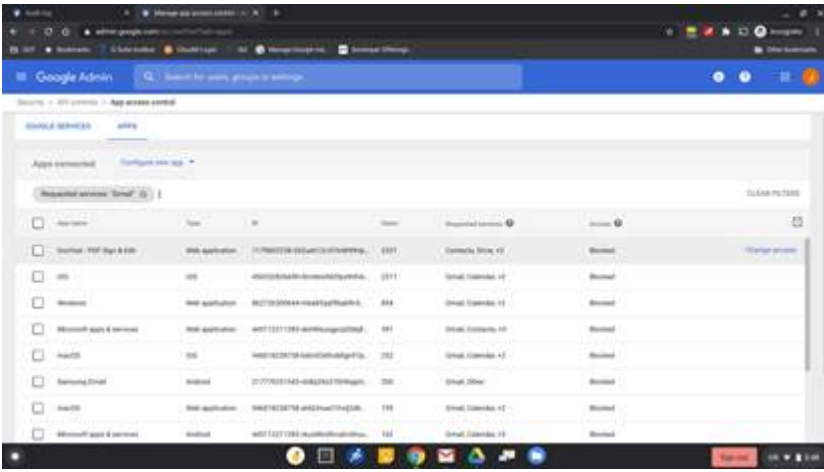
This was then applied to Gmail



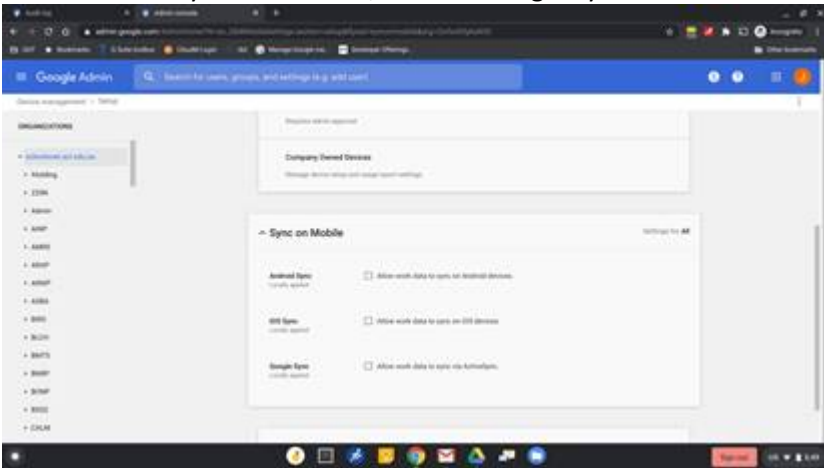
I also blocked OAuth access to Gmail



And all apps that are listed as blocked were trusted



I also disabled sync on Android, iOS and Google Sync

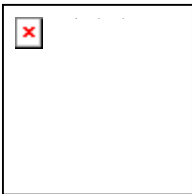
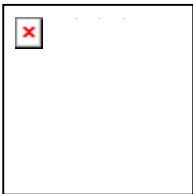


Cheers



[Redacted]  
[www.geeksontap.com.au](http://www.geeksontap.com.au)

p: 1300 885 489  
 e: [info@geeksontap.com.au](mailto:info@geeksontap.com.au)  
 w: [www.geeksontap.com.au](http://www.geeksontap.com.au)



Sydney | Melbourne | Brisbane



**CONFIDENTIALITY NOTICE:** This message transmission (including any accompanying documents) may contain information which is confidential and or privileged. As a result, if you are not the intended recipient, any dissemination, copying or action taken in reliance on the contents of the message is strictly prohibited.

Views expressed in this message are those of the sender rather than Geeks On Tap unless the content of the message indicates to the contrary.

If you have received this message in error you are requested to notify the sender and delete the message.

**From:** [Valtas, Julian](#)  
**To:** [Bayliss, Michael](#); [Williamson, Bill \(ACTEDU\)](#); [REDACTED]; [Bartlett, Kelly](#)  
**Cc:** [Ruecroft, Daniel](#); [McKay, Murray](#); [Sanderson, Mark](#); [Daniel, Ryan](#); [Carriage, Nathan](#); [Owen, Jonathan](#); [Blake, Al](#); [Hollis, Jeremy](#); [REDACTED]  
**Subject:** Re: Gmail DL Email incident [OFFICIAL]  
**Date:** Friday, 14 August 2020 7:54:09 PM  
**Attachments:** [image001.png](#)  
[image002.png](#)

---

Hi Michael,

I support your recommendation to Education as an option worth their strong consideration for phasing in re-enablement of the service (once offensive messages are purged): *An additional control which was suggested by Google was to block internal messages between [REDACTED] act.edu.au users, which could be useful in the case if we wanted to reopen access to Gmail but want to continue to restrict sending.*

Regards,  
 Julian Valtas  
 62071008

---

**From:** Bayliss, Michael <Michael.Bayliss@act.gov.au>  
**Sent:** Friday, August 14, 2020 7:38 pm  
**To:** Williamson, Bill (ACTEDU); [REDACTED]; Valtas, Julian; Bartlett, Kelly  
**Cc:** Ruecroft, Daniel; McKay, Murray; Sanderson, Mark; Daniel, Ryan; Carriage, Nathan; Owen, Jonathan; Blake, Al; Hollis, Jeremy; [REDACTED]  
**Subject:** RE: Gmail DL Email incident [OFFICIAL]

OFFICIAL: Sensitive

Hi Bill,

I think that is a good plan to ensure users are kicked out. It may also be possible to utilise the Bulk Upload feature in the Google Admin Console to achieve a similar outcome. We noticed some users being suspended and after checking with Murray we have disabled the Google user sync to ensure students are not inadvertently (automatically) re-enabled before you intend them to be.

An additional control which was suggested by Google was to block internal messages between @schoolsnet.act.edu.au users, which could be useful in the case if we wanted to reopen access to Gmail but want to continue to restrict sending. Happy to action this change if you would like.

Kind Regards,  
Michael

---

**From:** Williamson, Bill <Bill.Williamson@ed.act.edu.au>  
**Sent:** Friday, 14 August 2020 7:16 PM  
**To:** [REDACTED]@foresightconsulting.com.au>; Valtas, Julian <Julian.Valtas@act.gov.au>; Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
**Cc:** Ruecroft, Daniel <Daniel.Ruecroft@act.gov.au>; McKay, Murray <Murray.McKay@act.gov.au>; Sanderson, Mark <Mark.Sanderson@act.gov.au>; Daniel, Ryan <Ryan.Daniel@act.gov.au>; Bayliss, Michael <Michael.Bayliss@act.gov.au>; Carriage, Nathan <Nathan.Carriage@act.gov.au>; Owen, Jonathan <Jonathan.Owen@act.gov.au>; Blake, Al <Al.Blake@act.gov.au>; Hollis, Jeremy <Jeremy.Hollis@act.gov.au>; [REDACTED] <[REDACTED]@foresightconsulting.com.au>  
**Subject:** RE: Gmail DL Email incident [OFFICIAL]

Update ----

ACT Education are running a script to:

- List all non-suspended accounts
- Log them
- Suspend them

Suspending accounts will instantly kick a student off of any device (we have tested this).

Once this process is complete, we plan to:

- reenable authentication (will require SSICT)
- enable all services apart from email, groups, and device sync
- un-suspend accounts

Any thoughts by people on this list?

**Bill Williamson | Senior Director - School Administration System Architecture**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

**From:** [REDACTED] [@foresightconsulting.com.au](mailto:[REDACTED]@foresightconsulting.com.au)

**Sent:** Friday, 14 August 2020 6:45 PM

**To:** Valtas, Julian (ACTGOV) <[Julian.Valtas@act.gov.au](mailto:Julian.Valtas@act.gov.au)>; Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; Bartlett, Kelly (ACTGOV) <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>

**Cc:** Ruecroft, Daniel (ACTGOV) <[Daniel.Ruecroft@act.gov.au](mailto:Daniel.Ruecroft@act.gov.au)>; McKay, Murray (ACTGOV) <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Sanderson, Mark (ACTGOV) <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>; Daniel, Ryan (ACTGOV) <[Ryan.Daniel@act.gov.au](mailto:Ryan.Daniel@act.gov.au)>; Bayliss, Michael (ACTGOV) <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; Carriage, Nathan (ACTGOV) <[Nathan.Carriage@act.gov.au](mailto:Nathan.Carriage@act.gov.au)>; Owen, Jonathan (ACTGOV) <[Jonathan.Owen@act.gov.au](mailto:Jonathan.Owen@act.gov.au)>; Blake, Al (ACTGOV) <[Al.Blake@act.gov.au](mailto:Al.Blake@act.gov.au)>; Hollis, Jeremy (ACTGOV) <[Jeremy.Hollis@act.gov.au](mailto:Jeremy.Hollis@act.gov.au)>; [REDACTED] <[\[REDACTED\]@foresightconsulting.com.au](mailto:[REDACTED]@foresightconsulting.com.au)>

**Subject:** RE: Gmail DL Email incident [OFFICIAL]

**OFFICIAL**

Hi all,

Just outlining a high level list of actions that should be undertaken as part of this incident. If I could have access to review previous artefacts or documentation/status updates related to this ongoing incident, that would greatly assist with putting the assurance report together. Thanks to those that have already put some items together whilst I was drafting up this email.

- Ensure a timeline of the investigation is recorded and documented, covering incident triggers, investigation activities, containment and remediation actions undertaken.
- Ensure a regular incident response meeting or catch up is being undertaken to brief key stakeholders of the current status of action items and any new items that have been discovered.
  - Relevant executive stakeholders should also be included, particularly if key decisions need to be made in the incident such as temporarily disabling the email service, involving the Australian Federal Police (AFP) where content is deemed to be of sufficiently serious nature etc.
- Determine the infrastructure involved in the incident so that key evidence can be captured and where appropriate, containment and remediation actions can be performed.
  - At this point in time, it would appear to involve G-Suite and ContentKeeper. Please



- advise if other key systems have been highlighted as relevant to this incident.
- Logs should be exported ASAP from all systems involved, with at least one copy stored in read only form to ensure integrity.
    - Where possible the checksums of the files should be documented.
    - If escalation to the AFP does occur, then chain of custody needs to be considered.
  - Any backup media related to these systems should be marked for long term retention and if possible, stored offline, particularly if this becomes a matter for the courts.
  - Where licensed, Google Vault could be leveraged for data retention and eDiscovery.
  - A communications plan is developed outlining what stakeholders need to be addressed, what level of detail is to be provided and at what frequency.
    - Key stakeholders here may include internal staff, executive staff, related suppliers and service providers of the key systems, users of the key systems (e.g. when will access be restored), the general public and the media.
    - ACT Education may wish to consider advising the Australian Cyber Security Centre (ACSC) of this incident.
  - As part of the containment process ensure that:
    - All affected distribution lists have been identified that are vulnerable to mass emailing and have been reconfigured appropriately.
    - All user accounts identified to be partaking in the incident and/or actively attempting to circumvent containment controls to continue sending inappropriate emails should be disabled until further notice.
    - Access to the G suite service has been temporarily disabled while the investigation is underway.
      - Contact with all relevant service providers (such as Google) should be made to assist with the investigation and any containment measures required.
    - All potentially malicious content related to the mass emailing of distribution lists has been identified and removed from all affected G-Suite inboxes.
    - Identify all user accounts that were participating in a malicious manner.
    - If in the course of review, ACT Education discover content deemed to be of a sufficiently serious nature, the AFP may need to be engaged ASAP to assist in the investigation.
  - As part of the remediation process ensure that:
    - The root cause of the incident has been identified and understood.
    - No other misconfigured distribution lists exist in the environment that could be abused again.
    - Standard Operating Procedures (SOPs) have been updated so that internal staff securely configure all new distribution lists.
    - Review if ContentKeeper can be configured to provide filtering duties for internal emails where appropriate. E.g. student email content is checked for potentially malicious/inappropriate material.
    - Undertake a Post Incident Review (PIR) process to ensure the identified incident remediation actions have been undertaken, are effective and that any additional process/people/technology improvements are identified for similar incidents in the future.

Thanks,



[REDACTED]  
[REDACTED] [@foresightconsulting.com.au](mailto:[REDACTED]@foresightconsulting.com.au)



This message is intended for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. Any unauthorized use, distribution, or disclosure is strictly prohibited. If you have received this message in error, please notify sender immediately and destroy/delete the original transmission

OFFICIAL

Classified by [aostendorp@foresightconsulting.com.au](mailto:aostendorp@foresightconsulting.com.au) on 14/08/2020 6:44:30 PM

**From:** Valtas, Julian <[Julian.Valtas@act.gov.au](mailto:Julian.Valtas@act.gov.au)>  
**Sent:** Friday, 14 August 2020 6:20 PM  
**To:** Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>; [REDACTED] <[\[REDACTED\]@foresightconsulting.com.au](mailto:[REDACTED]@foresightconsulting.com.au)>  
**Cc:** Ruecroft, Daniel <[Daniel.Ruecroft@act.gov.au](mailto:Daniel.Ruecroft@act.gov.au)>; McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Sanderson, Mark <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>; Daniel, Ryan <[Ryan.Daniel@act.gov.au](mailto:Ryan.Daniel@act.gov.au)>; Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; Carriage, Nathan <[Nathan.Carriage@act.gov.au](mailto:Nathan.Carriage@act.gov.au)>; Owen, Jonathan <[Jonathan.Owen@act.gov.au](mailto:Jonathan.Owen@act.gov.au)>; Blake, Al <[Al.Blake@act.gov.au](mailto:Al.Blake@act.gov.au)>; Hollis, Jeremy <[Jeremy.Hollis@act.gov.au](mailto:Jeremy.Hollis@act.gov.au)>  
**Subject:** RE: Gmail DL Email incident

Thanks for the summary on your side Bill. I've looped a few other key staff in to this message from SSICT side, FYI.

Summary of actions taken on our end:

- Based on EDU request, provided an EDU staff member with super-user GSuite access and reset password for an existing EDU super-user account.
- Changed the configuration of groups that enabled broad distribution list functionality that was taken advantage in this incident.
- Disabled Google Mail on all student OU's (as distinct from the entire disablement that occurred later that Bill referred to).
- Disabled Google mail domains on the ContentKeeper internet filter. This prevented student access to known Google mail domains from school wifi/wired network from managed and unmanaged BYOD devices.
- Single sign on integration disabled,
- A number of Google Vault search/exports performed to capture evidence of offensive/inappropriate use of email system – these are still running and unlikely to yield any results for at least 24 hours given the volume of mail/number of mailboxes. These may be redundant in light of Bill highlighting this work having been performed on their side.
- Australian Cyber Security Centre advised of the incident.
- SSICT incident response team formed, ready to assist EDU/Foresight as required.

Regards,

**Julian Valtas** | Director, ICT Security Operations

Phone: +61 2 62071008 | Mobile: 0432131114

**Shared Services ICT | Chief Minister, Treasury and Economic Development Directorate | ACT Government**

Level 2, Winyu House, 125 Gungahlin Place, ACT | GPO Box 158 Canberra ACT 2601 |

[www.act.gov.au](http://www.act.gov.au)

**From:** Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>

**Sent:** Friday, 14 August 2020 5:59 PM

**To:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>; [REDACTED] <[\[REDACTED\]@foresightconsulting.com.au](mailto:[REDACTED]@foresightconsulting.com.au)>  
**Cc:** Rucroft, Daniel <[Daniel.Rucroft@act.gov.au](mailto:Daniel.Rucroft@act.gov.au)>; McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Sanderson, Mark <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>; Valtas, Julian <[Julian.Valtas@act.gov.au](mailto:Julian.Valtas@act.gov.au)>; Daniel, Ryan <[Ryan.Daniel@act.gov.au](mailto:Ryan.Daniel@act.gov.au)>  
**Subject:** RE: Gmail DL Email incident

Hi [REDACTED],

Just a quick recap of the work we (ACT Education) have done to mitigate thus far. This doesn't include additional actions taken by the SSICT team.

- Turned off the G-Mail service
- Turned off Google Groups Service
- Activated the investigation tool to audit the messages in question
- Added mail.google.com and groups.google.com to blocked urls in the chromebook management console
- Manually suspended several users who were creating new groups and sending emails through a cached login

Geeks On Tap (our google consultants) took the following actions:

- Enabled context away access to block gmail
- Blocked OAuth access to gmail
- Blocked trusted apps
- Disabled Sync for IOS/Android/Google Sync

SSICT took alternative actions which I will let them address, but included blocking services at the firewall layer and disabling authentication.

**Bill Williamson | Senior Director - School Administration System Architecture**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

---

**From:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>

**Sent:** Friday, 14 August 2020 5:03 PM

**To:** [REDACTED] <[\[REDACTED\]@foresightconsulting.com.au](mailto:[REDACTED]@foresightconsulting.com.au)>

**Cc:** Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; Rucroft, Daniel (ACTGOV) <[Daniel.Rucroft@act.gov.au](mailto:Daniel.Rucroft@act.gov.au)>; McKay, Murray (ACTGOV) <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Sanderson, Mark (ACTGOV) <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>; Valtas, Julian (ACTGOV) <[Julian.Valtas@act.gov.au](mailto:Julian.Valtas@act.gov.au)>; Daniel, Ryan (ACTGOV) <[Ryan.Daniel@act.gov.au](mailto:Ryan.Daniel@act.gov.au)>

**Subject:** Gmail DL Email incident

OFFICIAL: Sensitive

Hi [REDACTED]

As discussed, if you can please commence an independent assurance report on our approach to address this issue?

Please see copied technical team.

Summary - Earlier today we were notified of emails being sent by students to all schools year groups (all Year 9) Most are jokes and inappropriate one liners, however there are some of highly inappropriate pornographic.

We are still investigating logs etc to validate.

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government  
51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
[www.education.act.gov.au](http://www.education.act.gov.au)

-----  
This email, and any attachments, may be confidential and also privileged. If you are not the intended recipient, please notify the sender and delete all copies of this transmission along with any attachments immediately. You should not copy or use it for any purpose, nor disclose its contents to any other person.  
-----

## Caveat Brief

**To:** Minister for Education and Early Childhood Development  
**From:** Ross Hawkins – Executive Group manager Service Design and Delivery  
**Subject:** E-mail incident 14 August 2020  
**Date:** 14 August 2020

That you note the occurrence of an email incident on the Google platform and the measures taken by the Education Directorate to address it.

**Noted / Please discuss**

**Yvette Berry MLA..../..../....**

- On 14 August 2020, the Education Directorate was alerted to an email incident which occurred in ACT public schools. The incident involved inappropriate images being circulated to student email accounts.
- On notification to the EGM SDD, we moved to block access to the Google platform for all schools. This meant that students and schools would not be able to access the Google Suite for Education (GSFE) including email and the Google platform.
- The Education Directorate is investigating the cause of the incident. Preliminary indications are that this was not an external attack.
- It appears that students have discovered a group email distribution list based on year level and used these lists to distribute inappropriate materials in an escalating manner.
- The Education Directorate is confirming what content was distributed to which groups (e.g. what student cohorts had visibility of which email). It has been confirmed that some content distributed included inappropriate sexual content.
- As requested by your office, the Education Directorate has engaged an external provider (Foresight Consulting) to conduct a security review. The review will be conducted in two parts:
  - Part 1 - Confirm that the actions the Education Directorate have taken since the incident are appropriate, and the platform can now be un-blocked.
  - Part 2 - A more comprehensive review of what took place, and consideration for any similar vulnerabilities which exist in the system.
- Foresight Consulting will work over the weekend (15-16 August 2020) on Part 1 to provide assurance that the Education Directorate has taken appropriate steps to control the incident and that there are appropriate controls in place for schools to resume using the Google platform.
- Blocking the Google platform will impact the ability of students to study over the weekend using this platform. Schools will work with students and their families in relation to any impacts on assessment.

- Once the platform is unblocked, users may need to reset their passwords.
- Principals have been informed and provided with information to support their engagement with the families of impacted students.
- Families of impacted students are being provided with, links to conversation aids that are available through the eSafety Commissioner website.
- Relevant bodies have been notified in relation to this incident, including:
  - ACT Chief Digital Officer
  - AFP Online Child Safety Team
  - P&C Association
  - eSafety Commissioner
- The Education Directorate is liaising with Catholic Education and Independent Schools Association to ensure that they are aware of the possibility that their students may have been impacted by further circulation of the inappropriate material.
- A comprehensive chronology is being developed, including what was sent at what time. This will be developed over the weekend. The current chronology of events is provided at **Attachment A**.

Signatory Name: Ross Hawkins  
Title Executive Group Manager, Service  
Design and Delivery, Education  
Directorate  
Date 14 August 2020

## Attachment A – Chronology of events

<b>Time</b>	<b>Action</b>	<b>Description</b>
12.40hrs	Notification to EGMSDD	Executive General Manager, Service Design and Delivery was informed of an email incident which occurred in ACT public schools.  EGM SDD requested for the Google Platform to be shut down to ensure there was no further distribution of inappropriate emails.
12.40hrs	Preliminary investigation commenced	CIO was informed to commence investigation as to the nature of the incident.
13.00hrs	Scale of incident identified	EDU and Shared Services ICT identified that a large number of students were impacted by the email incident.
13.00hrs	Google access blocked	The Education Directorate, shut down all access to the Google Suite for Education for schools and students.
13.40hrs	ACT Chief Digital Officer notified	At approximately 13.40hrs the ACT Chief Digital Officer was notified of the email incident.
14.00hrs	eSafety Commissioner notified	At approximately 14.00hrs the Office of the eSafety Commissioner was notified of the email incident.
14.05hrs	P&C Association notified	At 14.05hrs the P&C Association was notified of the incident.
14.30hrs	AFP Online Child Safety Team notified	At 14.30hrs, Education Directorate staff notified the AFP Online Child Safety Team. Email confirmation of the notification was provided subsequently at 15.52hrs.
15.30hrs	Remaining Google users suspended	Google users who remained logged into their accounts had their access suspended.

**From:** [Williamson, Bill](#)  
**To:** [Bartlett, Kelly](#)  
**Subject:** FW: Group sync issues summary  
**Date:** Saturday, 15 August 2020 1:17:25 PM  
**Attachments:** [image001.png](#)

---

Important bit, the following groups all had this issue:

CN=internet-EDU-00A  
CN=internet-EDU-00B  
CN=internet-EDU-00K  
CN=internet-EDU-01  
CN=internet-EDU-02  
CN=internet-EDU-03  
CN=internet-EDU-04  
CN=internet-EDU-05  
CN=internet-EDU-06  
CN=internet-EDU-07  
CN=internet-EDU-08  
CN=internet-EDU-09  
CN=internet-EDU-10  
CN=internet-EDU-11  
CN=internet-EDU-12  
CN=internet-EDU-O  
CN=internet-EDU-O1  
CN=internet-EDU-O2  
O365AccessForStudents  
AdobeCloudAccessForStudents  
AdobeCreativeCloudAccessForStudents  
ClickviewAccessForStudents  
GoogleAccessForStudents  
GROKAccessForStudents

**Bill Williamson | Senior Director - School Administration System Architecture**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

[cid:image002.png@01D4E953.9786AC90](#)

---

**From:** Southwell, Mark <Mark.Southwell@act.gov.au>

**Sent:** Saturday, 15 August 2020 11:25 AM

**To:** Williamson, Bill <Bill.Williamson@ed.act.edu.au>; Bayliss, Michael (ACTGOV) <Michael.Bayliss@act.gov.au>

**Cc:** Blyth, Kylie (ACTGOV) <Kylie.Blyth@act.gov.au>; Bensley, Sara (ACTGOV) <Sara.Bensley@act.gov.au>

**Subject:** Group sync issues summary

OFFICIAL

Hi Bill,

As discussed on the phone the Internet groups and the application role groups were sourced via SAS data, and provisioned to LDAP (ADLDS), and then to Google via the Google Cloud Directory Sync (GCDS) utility. This is the same process used for class, year, role, and school groups. Groups



are then post processed via the GAM utility to apply different security, GAL listing settings, etc. I've investigated the sync process, the reason that these groups were in Google, and had default permissions is due to two issues:

1. In this instance these groups were not in any scope for permission post processing by GAM. Groups in scope of post processing are all groups matching the following criteria. These have been updated for new naming conventions for the new IDAM solution, however scope (group types) remains the same as the previous solution:

```
displayName=*_CLASS_*
displayName=*_ROLL_*
CN=*_YEAR_*
CN=*_SCHOOL
CN!=*_Staff
CN!=*_ITAdmins
```

2. These groups were marked for sync to Google due to having a "googleName" value populated in ADLDS. Previously (before the new IDAM solution) not all groups in ADLDS were synchronised to Google by GCDS. Sync criteria is below. Issue here is there isn't a mechanism in the new IDAM/Datahub to identify what groups from SAS need syncing to Google and what need to remain just in AD/ADLDS for on-prem services (web gateways, etc). Therefore these groups were synced just like class groups, etc.

With the previous solution, groups sourced from MAZE were synced to Google. Other groups, like the old IDAM\_Internet\_<year>\_<Schoolcode> groups, were not sourced via MAZE and therefore not synced to Google.

```
<groups>
<search>
<priority>1</priority>
<basedn>CN=Managed Groups,CN=Teachers,CN=Schools,DC=InTACT</basedn>
<scope>SUBTREE</scope>
<filter>(&(objectclass=group)(googleName=*)(ownersExpanded=*))</filter>
<memberAttrName>member</memberAttrName>
<groupIdentifierAttr>mail</groupIdentifierAttr>
<groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
<groupDescriptionAttribute>googleName</groupDescriptionAttribute>
<ownerDnAttribute>ownersExpanded</ownerDnAttribute>
<userEmailAttribute>mail</userEmailAttribute>
</search>
<search>
<priority>2</priority>
<basedn>CN=Managed Groups,CN=Students,CN=Schools,DC=InTACT</basedn>
<scope>SUBTREE</scope>
<filter>(&(objectclass=group)(googleName=*)(ownersExpanded=*))</filter>
<memberAttrName>member</memberAttrName>
<groupIdentifierAttr>mail</groupIdentifierAttr>
<groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
<groupDescriptionAttribute>googleName</groupDescriptionAttribute>
<ownerDnAttribute>ownersExpanded</ownerDnAttribute>
<userEmailAttribute>mail</userEmailAttribute>
</search>
<search>
```

```

<priority>3</priority>
<basedn>CN=Managed Groups,CN=Teachers,CN=Schools,DC=InTACT</basedn>
<scope>SUBTREE</scope>
<filter>(&!(objectclass=group)(googleName=*)!(ownersExpanded=*))</filter>
<memberAttrName>member</memberAttrName>
<groupIdentifierAttr>mail</groupIdentifierAttr>
<groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
<groupDescriptionAttribute>googleName</groupDescriptionAttribute>
<ownerLiteralAttribute>ownerMailAddresses</ownerLiteralAttribute>
<userEmailAttribute>mail</userEmailAttribute>
</search>
<search>
<priority>4</priority>
<basedn>CN=Managed Groups,CN=Students,CN=Schools,DC=InTACT</basedn>
<scope>SUBTREE</scope>
<filter>(&!(objectclass=group)(googleName=*)!(ownersExpanded=*)!(description=*))</filter>
<memberAttrName>member</memberAttrName>
<groupIdentifierAttr>mail</groupIdentifierAttr>
<groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
<groupDescriptionAttribute>googleName</groupDescriptionAttribute>
<ownerLiteralAttribute>ownerMailAddresses</ownerLiteralAttribute>
<userEmailAttribute>mail</userEmailAttribute>
</search>
<search>
<priority>5</priority>
<basedn>CN=Managed Groups,CN=Students,CN=Schools,DC=InTACT</basedn>
<scope>SUBTREE</scope>
<filter>(&!(objectclass=group)(googleName=*)!(ownersExpanded=*)(description=*))</filter>
<memberAttrName>member</memberAttrName>
<groupIdentifierAttr>mail</groupIdentifierAttr>
<groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
<groupDescriptionAttribute>description</groupDescriptionAttribute>
<ownerLiteralAttribute>ownerMailAddresses</ownerLiteralAttribute>
<userEmailAttribute>mail</userEmailAttribute>
</search>
</groups>

```

The groups below would be affected by this issue:

```

CN=internet-EDU-00A
CN=internet-EDU-00B
CN=internet-EDU-00K
CN=internet-EDU-01
CN=internet-EDU-02
CN=internet-EDU-03
CN=internet-EDU-04
CN=internet-EDU-05
CN=internet-EDU-06

```

CN=internet-EDU-07  
CN=internet-EDU-08  
CN=internet-EDU-09  
CN=internet-EDU-10  
CN=internet-EDU-11  
CN=internet-EDU-12  
CN=internet-EDU-O  
CN=internet-EDU-O1  
CN=internet-EDU-O2  
O365AccessForStudents  
AdobeCloudAccessForStudents  
AdobeCreativeCloudAccessForStudents  
ClickviewAccessForStudents  
GoogleAccessForStudents  
GROKAccessForStudents

Thanks,

**Mark Southwell MACS CP | Identity and Access Management**

Phone: 02 6207 6536 Mobile 0413 601729 | Email: [mark.southwell@act.gov.au](mailto:mark.southwell@act.gov.au)

**Shared Services | Chief Minister, Treasury and Economic Development Directorate | ACT Government**

Winyu House, Gungahlin | GPO Box 158, Canberra ACT 2601 | [act.gov.au](http://act.gov.au)

**From:** [REDACTED]  
**To:** [McKay, Murray](#)  
**Cc:** [Williamson, Bill \(ACTEDU\)](#); [Bartlett, Kelly](#); [Southwell, Mark](#); [Bayliss, Michael](#)  
**Subject:** Re: Google settings - ensuring groups don't get posted to  
**Date:** Saturday, 15 August 2020 9:08:57 PM

---

**CAUTION:** This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hi Murray,

Thanks for the update. Are you able to reachout to the support team or respond to the existing case and request for instructions on this functionality.

There are ways to stop posts via both Email and Web UI but as far as i have tested there is no impact on drive. The support team can provide step by step instructions and should be able to point you to the right API or GAM command that could help scale it.

Let me know how you go. If you are not getting the correct response from them, let me know via txt or email.

They are 24/7 and you have a premium support tier with the support team.

Regards,

On Sat, Aug 15, 2020 at 6:53 PM McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)> wrote:

Hi [REDACTED]

The root cause was the misuse of groups. Started with one student sharing a slides presentation with all of year 8 using a group. Students then realised the groups existed and 1 hour later messages were hitting all groups 01-12.

We think we have worked out the actions required to restrict this on an individual group level, but would value your insights about what group settings should look like and ways we can streamline this.

Thanks  
Murray

Get [Outlook for iOS](#)

---

**From:** [REDACTED] <[\[REDACTED\]@google.com](mailto:[REDACTED]@google.com)>  
**Sent:** Saturday, August 15, 2020 6:38:42 PM  
**To:** Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>  
**Cc:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>; McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Southwell, Mark <[Mark.Southwell@act.gov.au](mailto:Mark.Southwell@act.gov.au)>; Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>  
**Subject:** Re: Google settings - ensuring groups don't get posted to

**CAUTION:** This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hi Bill,

Gmail will not stop sharing functionality In Google drive. These are separate. As for sharing to groups, do you plan on disabling groups as well?

Without know the root cause of the incident, it's hard to advice on next steps or additional steps.

Regards,

On Sat, 15 Aug 2020, 1:11 pm Williamson, Bill, <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)> wrote:

Hi [redacted]

To confirm, if we turn on everything except gmail, Users will not be able to share docs from google docs to a group (that relies on email)?

Any other considerations?

Thanks

**Bill Williamson | Senior Director - School Administration System Architecture**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

cid:image002.png@01D4E953.9786AC90

-----  
This email, and any attachments, may be confidential and also privileged. If you are not the intended recipient, please notify the sender and delete all copies of this transmission along with any attachments immediately. You should not copy or use it for any purpose, nor disclose its contents to any other person.  
-----

--  
[redacted]  
Google For Education  
[redacted]



*Learning Never Stops - [Google Teacher Center](#)*

---

**From:** McKay, Murray <Murray.McKay@act.gov.au>  
**Sent:** Sunday, 16 August 2020 9:29 AM  
**To:** Bayliss, Michael <Michael.Bayliss@act.gov.au>  
**Cc:** Ruecroft, Daniel <Daniel.Ruecroft@act.gov.au>; Sanderson, Mark <Mark.Sanderson@act.gov.au>; Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
**Subject:** RE: Group sync issues summary

OFFICIAL

Thanks Michael!

**Murray McKay | Director, Digital Literacies**

T: +61 2 620 59756 | E: [murray.mckay@act.gov.au](mailto:murray.mckay@act.gov.au)  
Digital Strategy, Services & Transformation | Education | ACT Government  
51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#)

---

**From:** Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>  
**Sent:** Sunday, 16 August 2020 9:28 AM  
**To:** McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>  
**Cc:** Ruecroft, Daniel <[Daniel.Ruecroft@act.gov.au](mailto:Daniel.Ruecroft@act.gov.au)>; Sanderson, Mark <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>  
**Subject:** FW: Group sync issues summary

OFFICIAL

Hi Murray,

Some additional assurance/evidence of settings applied.

Yesterday I also checked and screenshotted each of the large groups access settings in the admin console, in a similar fashion to what we are doing today (although today we are focusing on the settings in the Groups themselves, and a wider range of settings, rather than admin console).

Cheers,  
Michael

---

**From:** Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>  
**Sent:** Saturday, 15 August 2020 8:44 PM  
**To:** Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>  
**Subject:** RE: Group sync issues summary

OFFICIAL

GoogleAccessForStudents

[googleaccessforstudents@\[REDACTED\]act.edu.au](mailto:googleaccessforstudents@[REDACTED]act.edu.au)



CUSTOM

# GoogleAccessForStudents

googleaccessforstudents@[redacted].act.edu.au

✎ RENAME GROUP

🗑 DELETE GROUP

## Settings

Access type

Moderation and advanced settings



ClickviewAccessForStudents  
[clickviewaccessforstudents@\[redacted\].act.edu.au](mailto:clickviewaccessforstudents@[redacted].act.edu.au)

The screenshot shows the Google Admin console interface. At the top, the browser address bar displays 'admin.google.com/ac/groups/017dp8vu3jqj8cw/settings'. Below this is the 'Google Admin' header with a search bar containing the text 'Search for users, groups or settings'. The breadcrumb navigation path is 'Groups > ClickviewAccessForStudents > Settings'. The main content area is split into two panels. The left panel, titled 'CUSTOM', displays the group name 'ClickviewAccessForStudents' and its email address 'clickviewaccessforstudents@[redacted].act.edu.au'. Below this are two action buttons: 'RENAME GROUP' with a pencil icon and 'DELETE GROUP' with a trash can icon. The right panel, titled 'Settings', shows the 'Access type' section, which is currently empty. At the bottom of the screenshot, a Windows taskbar is visible with icons for Outlook, Chrome, Teams, File Explorer, Excel, Edge, Task View, Word, and another File Explorer window.

O365AccessForStudents

CUSTOM

## 0365AccessForStudents

o365accessforstudents@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

Settings

Access type

Moderation and

GROKAccessForStudents  
[grokaccessforstudents\[REDACTED\].act.edu.au](http://grokaccessforstudents[REDACTED].act.edu.au)

CUSTOM

# GROKAccessForStudent

S

grokaccessforstudents@[redacted].act.edu.au

RENAME GROUP

DELETE GROUP

## Settings

Access type Custom

This acc

Access

Contact

View m

View to

Publish

Membe

Manage  
Add, inv

Who can  
Anyone

Allow m  
No

Moderation and advanced settings **Groups**

View an

AdobeCloudAccessForStudents  
[adobecloudaccessforstudents\[REDACTED\].act.edu.au](https://adobecloudaccessforstudents[REDACTED].act.edu.au)

CUSTOM

# AdobeCloudAccessForStudents

adobecloudaccessforstudents@  
act.edu.au

RENAME GROUP

DELETE GROUP

## Settings

Access type **Custom**  
This acc

Access s

Contact c

View me

View topi

Publish p

**Member**

Manage i  
Add, invit

**Who can**  
Anyone ir

**Allow me**  
No

Moderation and advanced settings **Groups f**  
View and

AdobeCreativeCloudAccessForStudents  
[adobecreativecloudaccessforstudents@\[REDACTED\].act.edu.au](mailto:adobecreativecloudaccessforstudents@[REDACTED].act.edu.au)



CUSTOM

# AdobeCreativeCloudAccessForStudents

adobecreativecloudaccessforstudents@  
act.edu.au

RENAME GROUP

DELETE GROUP

## Settings

Access type Custom  
This acc

Access :

Contact c

View me

View top

Publish p

Member

Manage |  
Add, invit

Who can  
Anyone i

Allow me  
No

Moderation and advanced settings Groups f  
View and

internet-EDU-00A

[internet-edu-00a@\[REDACTED\].act.edu.au](mailto:internet-edu-00a@[REDACTED].act.edu.au)

CUSTOM

# internet-EDU-00A

internet-edu-00a@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

## Settings

Access type Custom  
This ac

Access:

Contact

View m

View to

Publish

Membr

Manag  
Add, in

Who ca  
Anyone

Allow n  
No

Moderation and advanced settings **Groups**

View ar



internet-EDU-00B

[internet-edu-00b@\[REDACTED\].act.edu.au](mailto:internet-edu-00b@[REDACTED].act.edu.au)

CUSTOM

### internet-EDU-00B

internet-edu-00b@[redacted].act.edu.au

 RENAME GROUP

 DELETE GROUP

### Settings

Access type Custom  
This acc

Access

Contact

View me

View top

Publish

Membe

Manage  
Add, inv

Who can  
Anyone

Allow m  
No

Moderation and advanced settings Groups  
View an

internet-EDU-00K

[internet-edu-00k](#)  [act.edu.au](#)

CUSTOM

### internet-EDU-00K

internet-edu-00k@[redacted].act.edu.au

 RENAME GROUP

 DELETE GROUP

### Settings

Access type Custom  
This acc

Access

Contact

View m

View to

Publish

Membe

Manage  
Add, inv

Who ca  
Anyone

Allow r  
No

Moderation and advanced settings Groups  
View an



internet-EDU-01

[internet-edu-01@\[REDACTED\]act.edu.au](mailto:internet-edu-01@[REDACTED]act.edu.au)



CUSTOM

### internet-EDU-01

internet-edu-01@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

### Settings

Access type Custom  
This acc

Access

Contact

View me

View top

Publish j

Membe

Manage  
Add, invi

Who car  
Only invi

Allow m  
No

Moderation and advanced settings Groups f  
View an



internet-EDU-02

[internet-edu-02@\[REDACTED\]act.edu.au](mailto:internet-edu-02@[REDACTED]act.edu.au)

CUSTOM

# internet-EDU-02

internet-edu-02@[redacted]act.edu.au

✎ RENAME GROUP

🗑 DELETE GROUP

## Settings

Access type Custom  
This acc

Access s

Contact c

View mer

View topi

Publish p

Member

Manage i  
Add, invit

Who can  
Anyone ir

Allow me  
No

Moderation and advanced settings Groups fo  
View and



internet-EDU-03

[internet-edu-03@\[REDACTED\]act.edu.au](mailto:internet-edu-03@[REDACTED]act.edu.au)

CUSTOM

### internet-EDU-03

internet-edu-03@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

### Settings

Access type Custom  
This ac

Acces

Contact

View m

View tr

Publisl

Memb

Manag  
Add, in

Who c  
Anyone

Allow r  
No

Moderation and advanced settings Groups

View a

internet-EDU-04

[internet-edu-04@\[REDACTED\].act.edu.au](mailto:internet-edu-04@[REDACTED].act.edu.au)

CUSTOM

# internet-EDU-04

internet-edu-04@[redacted]act.edu.au

RENAME GROUP

DELETE GROUP

## Settings

Access type Custom  
This access

Access set

Contact ow

View memb

View topics

Publish pos

### Membersh

Manage me  
Add, invite, i

Who can joi  
Anyone in tl

Allow meml  
No

Moderation and advanced settings Groups for l  
View and ec



# internet-EDU-05

[internet-edu-05](#)  [act.edu.au](#)



CUSTOM

# internet-EDU-05

internet-edu-05 [redacted]act.edu.au

RENAME GROUP

DELETE GROUP

## Settings

Access type Custom  
This acc

Access

Contact

View m

View to

Publish

Membe

Manage  
Add, inv

Who ca  
Anyone

Allow n  
No

Moderation and advanced settings Groups  
View an



internet-EDU-06

[internet-edu-06](#) [REDACTED] [.act.edu.au](#)

CUSTOM

# internet-EDU-06

internet-edu-06@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

## Settings

Access type Custom  
This acc

Access

Contact

View me

View top

Publish p

Member

Manage  
Add, invi

Who can  
Anyone i

Allow m  
No

Moderation and advanced settings Groups f  
View anc

internet-EDU-07

[internet-edu-07@\[REDACTED\].act.edu.au](mailto:internet-edu-07@[REDACTED].act.edu.au)

CUSTOM

# internet-EDU-07

internet-edu-07@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

## Settings

Access type Custom  
This acc

Access s

Contact c

View me

View topi

Publish p

### Member

Manage i  
Add, invit

Who can  
Anyone in

Allow me  
No

Moderation and advanced settings Groups f  
View and

internet-EDU-08

[internet-edu-08](#)  [.act.edu.au](#)

CUSTOM

### internet-EDU-08

internet-edu-08@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

### Settings

Access type Custom  
This acco

Access :

Contact (

View me

View top

Publish p

#### Member

Manage |  
Add, invit

Who can  
Anyone i

Allow me  
No

Moderation and advanced settings Groups f  
View and

internet-EDU-09

[internet-edu-09@\[REDACTED\]act.edu.au](mailto:internet-edu-09@[REDACTED]act.edu.au)



CUSTOM

# internet-EDU-09

internet-edu-09@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

## Settings

Access type Custom  
This acc

Access

Contact

View me

View top

Publish

Member

Manage  
Add, invi

Who can  
Anyone i

Allow m  
No

Moderation and advanced settings Groups f  
View anc

internet-EDU-10

[internet-edu-10@\[REDACTED\]act.edu.au](mailto:internet-edu-10@[REDACTED]act.edu.au)

CUSTOM

# internet-EDU-10

internet-edu-10@act.edu.au

 RENAME GROUP

 DELETE GROUP

## Settings

Access type Custom  
This acce

Access s

Contact c

View mer

View topi

Publish p

Member:

Manage r  
Add, invit

Who can  
Anyone ir

Allow me  
No

Moderation and advanced settings [Groups fo](#)

View and

internet-EDU-11

[internet-edu-11@\[REDACTED\].act.edu.au](mailto:internet-edu-11@[REDACTED].act.edu.au)



CUSTOM

# internet-EDU-11

internet-edu-11@[redacted]act.edu.au

RENAME GROUP

DELETE GROUP

## Settings

Access type Custom  
This acc

### Access

Contact

View me

View top

Publish

### Membe

Manage  
Add, inv

Who can  
Anyone

Allow m  
No

Moderation and advanced settings Groups  
View an

internet-EDU-12

[internet-edu-12@\[REDACTED\]act.edu.au](mailto:internet-edu-12@[REDACTED]act.edu.au)

CUSTOM

# internet-EDU-12

internet-edu-12@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

## Settings

Access type Custom  
This acco

Access :

Contact (

View me

View top

Publish p

### Member

Manage |  
Add, invit

Who can  
Anyone i

Allow me  
No

Moderation and advanced settings Groups f  
View and

internet-EDU-O

[internet-edu-o@\[REDACTED\].act.edu.au](mailto:internet-edu-o@[REDACTED].act.edu.au)



CUSTOM

# internet-EDU-O

internet-edu-o@[redacted]act.edu.au

✎ RENAME GROUP

🗑 DELETE GROUP

## Settings

Access type Custom  
This acc

Access

Contact

View me

View top

Publish j

Membe

Manage  
Add, invi

Who can  
Anyone i

Allow m  
No

Moderation and advanced settings Groups f

View anc

internet-EDU-O1

[internet-edu-o1@\[REDACTED\].act.edu.au](mailto:internet-edu-o1@[REDACTED].act.edu.au)

CUSTOM

# internet-EDU-01

internet-edu-01@[redacted].act.edu.au

 RENAME GROUP

 DELETE GROUP

## Settings

Access type Custom  
This acc

Access

Contact

View me

View top

Publish j

Membe

Manage  
Add, invi

Who can  
Anyone i

Allow m  
No

Moderation and advanced settings Groups f  
View anc

internet-EDU-O2

[internet-edu-o2@\[REDACTED\]act.edu.au](mailto:internet-edu-o2@[REDACTED]act.edu.au)

CUSTOM

# internet-EDU-02

internet-edu-02@[redacted]act.edu.au

 RENAME GROUP

 DELETE GROUP

## Settings

Access type Custom  
This acc

Access s

Contact c

View mer

View topi

Publish p

### Member

Manage i  
Add, invit

Who can  
Anyone in

Allow me  
No

Moderation and advanced settings Groups f  
View and

**From:** Southwell, Mark <[Mark.Southwell@act.gov.au](mailto:Mark.Southwell@act.gov.au)>  
**Sent:** Saturday, 15 August 2020 11:25 AM  
**To:** Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>  
**Cc:** Blyth, Kylie <[Kylie.Blyth@act.gov.au](mailto:Kylie.Blyth@act.gov.au)>; Bensley, Sara <[Sara.Bensley@act.gov.au](mailto:Sara.Bensley@act.gov.au)>  
**Subject:** Group sync issues summary

## OFFICIAL

Hi Bill,

As discussed on the phone the Internet groups and the application role groups were sourced via SAS data, and provisioned to LDAP (ADLDS), and then to Google via the Google Cloud Directory Sync (GCDS) utility. This is the same process used for class, year, role, and school groups. Groups are then post processed via the GAM utility to apply different security, GAL listing settings, etc.

I've investigated the sync process, the reason that these groups were in Google, and had default permissions is due to two issues:

1. In this instance these groups were not in any scope for permission post processing by GAM. Groups in scope of post processing are all groups matching the following criteria. These have been updated for new naming conventions for the new IDAM solution, however scope (group types) remains the same as the previous solution:

```
displayName=*_CLASS_*
displayName=*_ROLL_*
CN=*_YEAR_*
CN=*_SCHOOL
CN!=*_Staff
CN!=*_ITAdmins
```

2. These groups were marked for sync to Google due to having a "googleName" value populated in ADLDS. Previously (before the new IDAM solution) not all groups in ADLDS were synchronised to Google by GCDS. Sync criteria is below. Issue here is there isn't a mechanism in the new IDAM/Datahub to identify what groups from SAS need syncing to Google and what need to remain just in AD/ADLDS for on-prem services (web gateways, etc). Therefore these groups were synced just like class groups, etc.

With the previous solution, groups sourced from MAZE were synced to Google. Other groups, like the old IDAM\_Internet\_<year>\_<Schoolcode> groups, were not sourced via MAZE and therefore not synced to Google.

```
<groups>
  <search>
    <priority>1</priority>
    <basedn>CN=Managed Groups,CN=Teachers,CN=Schools,DC=InTACT</basedn>
    <scope>SUBTREE</scope>
    <filter>(&(objectclass=group)(googleName=*)(ownersExpanded=*))</filter>
    <memberAttrName>member</memberAttrName>
    <groupIdentifierAttr>mail</groupIdentifierAttr>
    <groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
    <groupDescriptionAttribute>googleName</groupDescriptionAttribute>
    <ownerDnAttribute>ownersExpanded</ownerDnAttribute>
    <userEmailAttribute>mail</userEmailAttribute>
```

```

</search>
<search>
  <priority>2</priority>
  <basedn>CN=Managed Groups,CN=Students,CN=Schools,DC=InTACT</basedn>
  <scope>SUBTREE</scope>
  <filter>(&amp;(objectclass=group)(googleName=*)(ownersExpanded=*))</filter>
  <memberAttrName>member</memberAttrName>
  <groupIdentifierAttr>mail</groupIdentifierAttr>
  <groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
  <groupDescriptionAttribute>googleName</groupDescriptionAttribute>
  <ownerDnAttribute>ownersExpanded</ownerDnAttribute>
  <userEmailAttribute>mail</userEmailAttribute>
</search>
<search>
  <priority>3</priority>
  <basedn>CN=Managed Groups,CN=Teachers,CN=Schools,DC=InTACT</basedn>
  <scope>SUBTREE</scope>
  <filter>(&amp;(objectclass=group)(googleName=*)(!(ownersExpanded=*))</filter>
  <memberAttrName>member</memberAttrName>
  <groupIdentifierAttr>mail</groupIdentifierAttr>
  <groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
  <groupDescriptionAttribute>googleName</groupDescriptionAttribute>
  <ownerLiteralAttribute>ownerMailAddresses</ownerLiteralAttribute>
  <userEmailAttribute>mail</userEmailAttribute>
</search>
<search>
  <priority>4</priority>
  <basedn>CN=Managed Groups,CN=Students,CN=Schools,DC=InTACT</basedn>
  <scope>SUBTREE</scope>
  <filter>(&amp;(objectclass=group)(googleName=*)(!(ownersExpanded=*))(!(description=*))</filter>
  <memberAttrName>member</memberAttrName>
  <groupIdentifierAttr>mail</groupIdentifierAttr>
  <groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
  <groupDescriptionAttribute>googleName</groupDescriptionAttribute>
  <ownerLiteralAttribute>ownerMailAddresses</ownerLiteralAttribute>
  <userEmailAttribute>mail</userEmailAttribute>
</search>
<search>
  <priority>5</priority>
  <basedn>CN=Managed Groups,CN=Students,CN=Schools,DC=InTACT</basedn>
  <scope>SUBTREE</scope>
  <filter>(&amp;(objectclass=group)(googleName=*)(!(ownersExpanded=*))</filter>
  <memberAttrName>member</memberAttrName>
  <groupIdentifierAttr>mail</groupIdentifierAttr>
  <groupDisplayNameAttribute>googleName</groupDisplayNameAttribute>
  <groupDescriptionAttribute>description</groupDescriptionAttribute>
  <ownerLiteralAttribute>ownerMailAddresses</ownerLiteralAttribute>
  <userEmailAttribute>mail</userEmailAttribute>
</search>
</groups>

```

The groups below would be affected by this issue:

CN=internet-EDU-00A  
CN=internet-EDU-00B

CN=internet-EDU-00K  
CN=internet-EDU-01  
CN=internet-EDU-02  
CN=internet-EDU-03  
CN=internet-EDU-04  
CN=internet-EDU-05  
CN=internet-EDU-06  
CN=internet-EDU-07  
CN=internet-EDU-08  
CN=internet-EDU-09  
CN=internet-EDU-10  
CN=internet-EDU-11  
CN=internet-EDU-12  
CN=internet-EDU-O  
CN=internet-EDU-O1  
CN=internet-EDU-O2

O365AccessForStudents  
AdobeCloudAccessForStudents  
AdobeCreativeCloudAccessForStudents  
ClickviewAccessForStudents  
GoogleAccessForStudents  
GROKAccessForStudents

Thanks,

**Mark Southwell MACS CP | Identity and Access Management**

Phone: 02 6207 6536 Mobile 0413 601729 | Email: [mark.southwell@act.gov.au](mailto:mark.southwell@act.gov.au)

**Shared Services | Chief Minister, Treasury and Economic Development Directorate | ACT Government**

Winyu House, Gungahlin | GPO Box 158, Canberra ACT 2601 | [act.gov.au](http://act.gov.au)



From: [Kelly, Kelly](#)  
To: [Bayliss, Michael](#), [Williamson, Bill](#), [ACTEDU](#)  
Cc: [Ruecroft, Daniel](#), [Sanderson, Mark](#), [McKay, Murray](#)  
Subject: RE: Google Drive - Students - ability to create new shared drives disabled  
Date: Sunday, 16 August 2020 4:00:00 PM  
Attachments: [image002.png](#)  
[image003.png](#)

OFFICIAL

Fabulous!!! Thank you so much!

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)  
Digital Strategy, Services & Transformation | Education | ACT Government  
51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
[www.education.act.gov.au](http://www.education.act.gov.au)

From: Bayliss, Michael <Michael.Bayliss@act.gov.au>

Sent: Sunday, 16 August 2020 5:55 PM

To: Williamson, Bill (ACTEDU) <Bill.Williamson@ed.act.edu.au>; Bartlett, Kelly <kelly.bartlett@act.gov.au>

Cc: Ruecroft, Daniel <Daniel.Ruecroft@act.gov.au>; Sanderson, Mark <Mark.Sanderson@act.gov.au>; McKay, Murray <Murray.McKay@act.gov.au>

Subject: Google Drive - Students - ability to create new shared drives disabled

OFFICIAL

Hi Bill & Kelly,

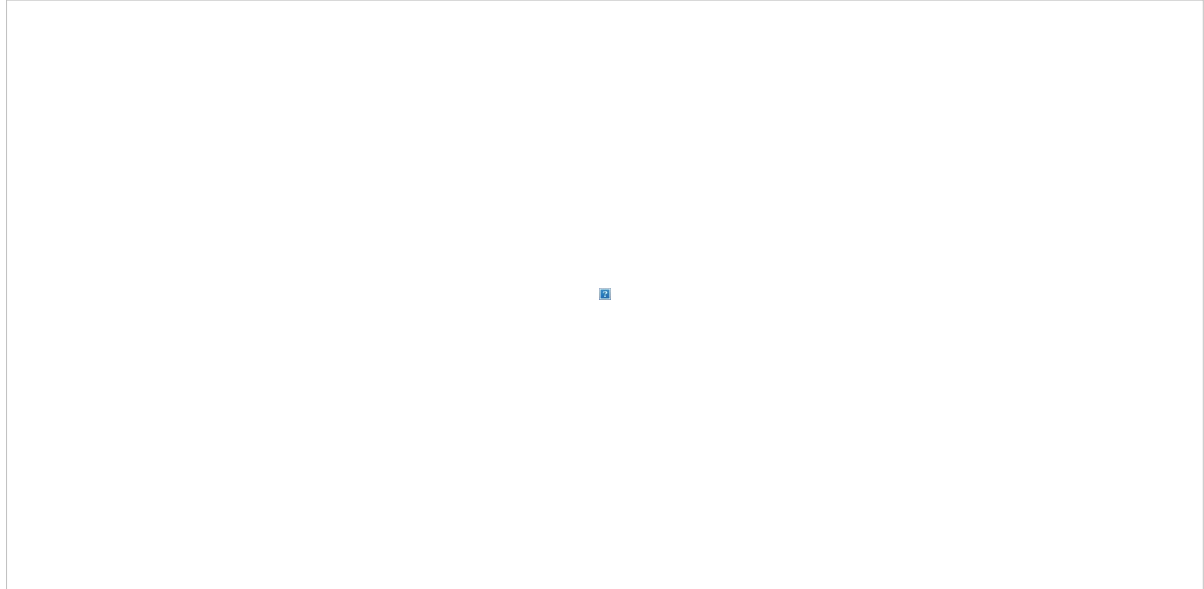
Quick follow up email to confirm the ability for students to create shared drives has been turned off in the Admin Console. Setting has been applied per-student OU, so staff will not be affected by this change.

- "Prevent users in All\_Students from creating new shared drives" changed from OFF to ON
- Other shared drive creation settings left unchanged from pre-existing

Example screenshot below showing settings applied.

Kind Regards,

Michael



Michael Bayliss | Assistant Director

Phone: +61 2 6205 9451

Customer Engagement Services Branch | Shared Services ICT | Chief Minister, Treasury and Economic Development | ACT Government

51 Fremantle Drive, Stirling, ACT 2611 | GPO Box 158 Canberra ACT 2601 | [www.act.gov.au](http://www.act.gov.au)

*Please consider the environment before printing this email. If printing is necessary, print double-sided and black and white.*

admin.google.com/ac/appsettings/55656082996/sharing

Google Admin Search for users, groups or settings

Apps > G Suite > Settings for Drive and Docs > Sharing settings

### Drive and Docs

- Users
- Groups
- Organisational units
- all\_students
  - schoolsnet.act.edu.au
    - AINP
      - All\_Students
    - AMRS
      - All\_Students
    - ARAP
      - All\_Students
    - ARWP
      - All\_Students
    - BLCH
      - All\_Students

#### Sharing options

Overridden

Sharing outside of ACT Education Directorate  
ON - Files owned by users in All\_Students can be shared outside of ACT Education Directorate.

Access Checker  
Recipients only, ACT Education Directorate, or public (no Google account required).

Distributing content outside of ACT Education Directorate  
Anyone

#### Shared drive creation

Overridden

- Prevent users in All\_Students from creating new shared drives
- Prevent full-access members from modifying shared drive settings
- Prevent people outside ACT Education Directorate from accessing files in the shared drive
- Prevent non-members of the shared drive from accessing files in the shared drive
- Prevent commenters and viewers from downloading, copying and printing files in the shared drive

*i* Changes may take up to 24 hours to propagate to all users.  
Prior changes can be seen in [Audit log](#)

INHERIT CANCEL SAVE

#### Link Sharing

Link Sharing Defaults

**From:** [Williamson, Bill](#)  
**To:** [redacted] [McKay, Murray](#)  
**Cc:** [Bartlett, Kelly](#)  
**Subject:** RE: Additional question - purging content [OFFICIAL]  
**Date:** Monday, 17 August 2020 11:19:53 AM  
**Attachments:** [image002.png](#)  
[image003.png](#)

Hi [redacted]  
We are evaluating different options, but Kelly has indicated we should not put effort into gmail until other services are resolved, as we are leaving gmail completely off.  
We are considering a range of options with various risk levels, but aren't actively working on it in detail at this point.

**Bill Williamson | Senior Director - School Administration System Architecture**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)  
Digital Strategy, Services & Transformation | Education | ACT Government  
51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)  
cid:image002.png@01D4E953.9786AC90

---

**From:** [redacted]@foresightconsulting.com.au>  
**Sent:** Monday, 17 August 2020 11:15 AM  
**To:** McKay, Murray (ACTGOV) <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>  
**Cc:** Bartlett, Kelly (ACTGOV) <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>  
**Subject:** Additional question - purging content [OFFICIAL]

**OFFICIAL**

Hi Murray & Bill,  
Just confirming the approach for purging inappropriate content from all email accounts. Am I able to get some bullet points on what is being done for this?  
I am assuming that it has been based off the initial log investigation (who started each mass email thread) and manually purging these email threads via the unique message ids?  
Thanks,

[redacted]  
[redacted] [@foresightconsulting.com.au](mailto:[redacted]@foresightconsulting.com.au)



This message is intended for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. Any unauthorized use, distribution, or disclosure is strictly prohibited. If you have received this message in error, please notify sender immediately and destroy/delete the original transmission

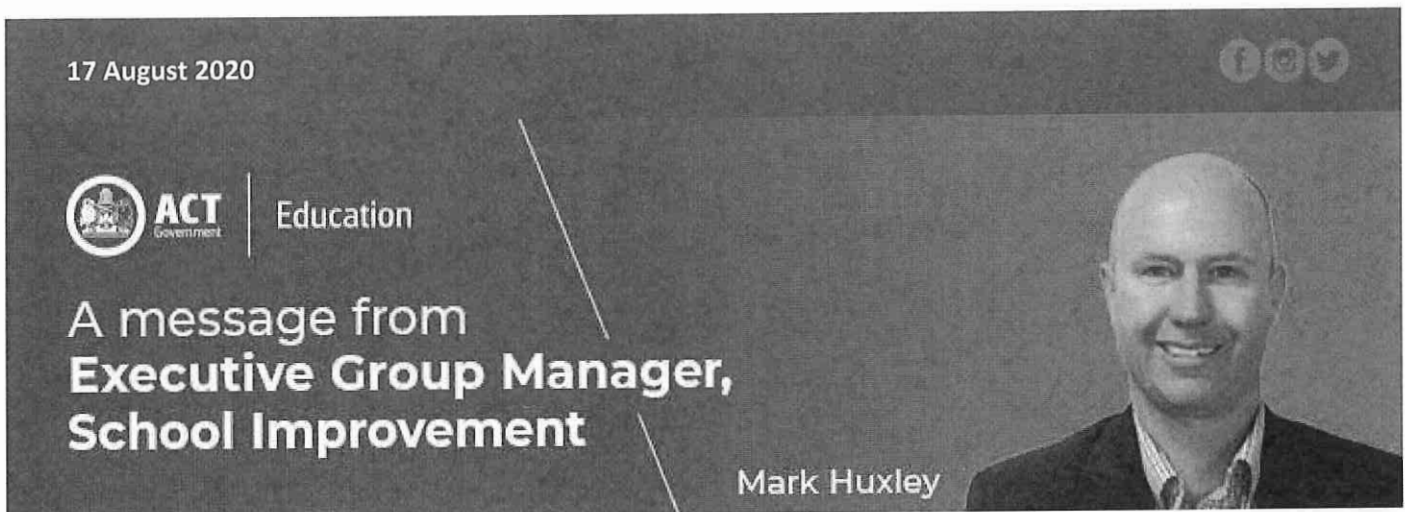
**OFFICIAL**

Classified by [redacted] [@foresightconsulting.com.au](mailto:[redacted]@foresightconsulting.com.au) on 17/08/2020 11:14:52 AM

**Fitzgibbon, Breanna**

**From:** EDU Alerts  
**Sent:** Monday, 17 August 2020 12:30 PM  
**To:** #EDU, School Leaders  
**Cc:** '##School Business Managers'  
**Subject:** A message from Executive Group Manager School Improvement: Principal email 17 August 2020  
**Attachments:** Parent carer update on email incident 170820.docx; Parent carer letter re email incident 140820.docx; Teacher eSafety resources - all years.pdf; Principal telecon script Final.docx

UNCLASSIFIED For-Official-Use-Only



Dear Principals

Thank you for making the time to join our early teleconference this morning.

You will have seen an email from the Director General last night including the Minister's statement, which provide the latest advice about our investigation into Friday's student email incident.

For further background please find attached:

- A copy of the letter to parents and carers from Katy Haire, which is **being sent via SAS today**
- A copy of the letter to parents and carers, **sent via SAS on Friday 14 August**
- Teacher resources for various year levels, to support discussion and learning about this incident
- My talking points from this morning's teleconference.

A reminder that we have also set up a survey form for you to provide any specific feedback or questions on this issue so we can track incidents and ensure supports are in place.

Thank you once again. I appreciate your understanding and support as we navigate this issue with our school communities.

Warm regards  
Mark Huxley  
Executive Group Manager, School Improvement

Read the latest ACT Public Schools news [HERE](#)

Follow us on



RESPECT INTEGRITY  
COLLABORATION  
INNOVATION



Dear Parent/Carer

On Friday 14 August, ACT public schools experienced an email incident, involving students accessing email distribution lists and circulating a range of material, including inappropriate content.

The Education Directorate blocked student access to the Google platform, including Gmail, while we commenced an urgent investigation.

Our investigation has confirmed no external body has hacked or exported information from our systems. The incident occurred when a student attempted to share their work with their classmates, accidentally using a global distribution list code. Other students 'replied all' and a small number of students shared inappropriate content, including pornographic imagery. This content was shared from their private devices as explicit content cannot be accessed from within the ACT public school's network.

We commend the students who deleted the emails and those who requested for content to stop being sent.

We have notified both the AFP and the eSafety Commissioner about this incident. The eSafety Commissioner website has an extensive range of free resources for parents and children: <https://www.esafety.gov.au/>.

Over the weekend we have worked to remove access to global distribution lists and rigorously test our systems to ensure students cannot again access the lists. An external consultant is providing independent oversight to ensure the ongoing safety of our Google platform.

We expect students will regain access to Google Drive and Google Classroom from Tuesday 18 August and access to their email accounts by the end of this week.

I understand that this incident has caused some anxiety for some students and families and that it has disrupted students being able to study effectively during this time. Schools will accommodate student needs where this incident has impacted on their scheduled assessments.

I am also conscious that some of the material in the emails may have been distressing for your child. Schools will support students and their families as required. Please talk to your school who can assist with any needs you may have, including facilitating sessions with school psychologists where required.

We also understand there have been some instances of bullying and harassment related to this incident. Please contact either your school or the Education Directorate so that we can support you and your family, and so that action can be taken.

Students and families can also access support services through KidsHelpline 1800 551 800 or lifeline 13 11 14.

If you wish to raise any concerns with the ACT Education Directorate about this issue, please contact our Families and Students, Complaints and Feedback Unit online via the [ACT Education Directorate contact form](#) or by phone [\(02\) 6205 5429](#).

The safety and wellbeing of your student remains our primary concern. We apologise for any inconvenience or distress caused by this incident.

Yours sincerely,

Katy Haire  
Director-General  
Education Directorate  
17 August 2020

Dear parent/carer

ACT public schools experienced an e-mail incident today which involved spam emails containing inappropriate material being circulated to students.

The Education Directorate has responded by temporarily blocking access to the Google platform which includes Gmail, Google drive and Google classroom. This platform will be unavailable until the incident has been investigated and appropriate controls are put in place. We understand this may impact some students' ability to study over the weekend and schools will take this into consideration, where appropriate.

An investigation has commenced to identify the cause of the incident and any additional implications.

We are aware that some students have copied emails to their personal devices, we would encourage you to speak with your child and have them delete any content. If you require support talking to your child about this incident, additional information is available through the eSafety Commissioner: <https://www.esafety.gov.au/parents>

If you wish to raise any concerns with the ACT Education Directorate about this issue, please contact our Families and Students, Complaints and Feedback Unit online via the [ACT Education Directorate contact form](#) or by phone [\(02\) 6205 5429](#).

Students and families can access support services through KidsHelpline 1800 551 800 or lifeline 13 11 14.

We are sorry for any inconvenience or impact that this may have caused you and your family.

The Directorate will keep you updated on the resolution of this incident.

Regards

Education Directorate

14 August 2020



**From:** [Bartlett, Kelly](#)  
**To:** [Haire, Katy](#); [DGEDUoffice](#); [Hawkins, Ross](#); [EGMSDD](#); [Matthews, David](#); [DDGEDUoffice](#)  
**Subject:** FW: Initial analysis of incident approach and Phase One enabling of services [OFFICIAL]  
**Date:** Monday, 17 August 2020 4:30:11 PM  
**Attachments:** [image001.png](#)  
[image002.png](#)

---

OFFICIAL: Sensitive

Hi All

Please see Foresight assurance below.

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)

---

**From:** [REDACTED]@foresightconsulting.com.au>

**Sent:** Monday, 17 August 2020 3:35 PM

**To:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>

**Cc:** [REDACTED]@foresightconsulting.com.au>

**Subject:** Initial analysis of incident approach and Phase One enabling of services [OFFICIAL]

**CAUTION:** This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

OFFICIAL

Hi Kelly,

Foresight have reviewed and assessed ACT Education's incident management approach in response to the email incident. The containment and recovery of services approach, controls and testing undertaken since the event are considered appropriate for ACT Education's Phase One plan to re-enable Google for Education services with the exception of Gmail.

Based on our assessment, several areas for improvement exist in the environment that should be considered prior to Phase Two (enabling Gmail service) and for long term management of the environment. Further advice will be provided to support the implementation of Phase Two.

Regards,

[REDACTED]

[REDACTED]@foresightconsulting.com.au



This message is intended for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. Any unauthorized use, distribution, or disclosure is strictly prohibited. If you have received this message in error, please notify sender immediately and destroy/delete the original transmission

OFFICIAL

Classified by [REDACTED]@foresightconsulting.com.au on 17/08/2020 3:34:48 PM

**From:** [REDACTED]  
**To:** [Williamson, Bill \(ACTEDU\)](mailto:Williamson.Bill@act.edu.au)  
**Cc:** [Bartlett, Kelly](mailto:Bartlett.Kelly@act.gov.au); [McKay, Murray](mailto:McKay.Murray@act.gov.au)  
**Subject:** Re: Problems with Rate Limits  
**Date:** Monday, 17 August 2020 8:27:20 PM  
**Attachments:** [image001.png](#)  
[image001.png](#)

**CAUTION:** This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

I'll share this with the team.

On Mon, 17 Aug 2020, 7:50 pm Williamson, Bill, <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)> wrote:

Hi, the project ID is 172677452673

This is fairly urgent, as it's preventing us from updating/unsuspending our users.

**Bill Williamson | Senior Director - School Administration System Architecture**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

cid:image002.png@01D4E953.9786AC90

**From:** [REDACTED] <[\[REDACTED\]@google.com](mailto:[REDACTED]@google.com)>  
**Sent:** Monday, 17 August 2020 6:25 PM  
**To:** Bartlett, Kelly (ACTGOV) <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>  
**Cc:** [REDACTED] <[\[REDACTED\]@google.com](mailto:[REDACTED]@google.com)>; [REDACTED] <[\[REDACTED\]@google.com](mailto:[REDACTED]@google.com)>; Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; McKay, Murray (ACTGOV) <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>  
**Subject:** Re: Problems with Rate Limits

Hi Kelly, thanks for checking in.

Bill: is there a project id associated with this? We might be able to explore raising the limits for a certain time.

Regards,

[REDACTED]

On Mon, 17 Aug 2020, 6:09 pm Bartlett, Kelly, <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)> wrote:

**OFFICIAL**

Hi [REDACTED]

Bill is having a number of issues with scripts to complete certain jobs. Current attempting to run scripts using API and the rate limits is slow and sometimes the jobs are crashing the job. We have been advised by Google support that one we don't have API support, plus this is an expected feature to protect Googles performance, by slowing and blocking large jobs.

Is there anything we can do to give us a window to reactive the accounts?

We are currently trying to finish setting things ups so we can activate all services except Gmail.

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)

-----  
This email, and any attachments, may be confidential and also privileged. If you are not the intended recipient, please notify the sender and delete all copies of this transmission along with any attachments immediately. You should not copy or use it for any purpose, nor disclose its contents to any other person.  
-----

## Education Directorate

UNCLASSIFIED

To: Director-General

Tracking No.: [Click here to enter text.](#)

Date: 17/08/2020

CC: Executive Group Manager, Service Design and Delivery  
Executive Group Manager, School ImprovementFrom: A/g Executive Branch Manager, Chief Information Officer, Digital Strategy,  
Services and TransformationSubject: Inappropriate Email Distribution ICT response: Phase One - approach to  
restoring G Suite (excluding Gmail) services for schools

Critical Date: 17/08/2020

Critical Reason: To provide confidence to enable the reinstatement of the system

- DDG .../.../...
- EBM .../.../...

**Recommendations**

That you:

1. Note the information contained in this brief;

**Noted / ~~Please Discuss~~**

2. Agree to a two phased approach for the reactivation of the Google platform and Gmail for ACT public schools

**Agreed / ~~Not Agreed~~ / ~~Please Discuss~~**

3. Agree to Phase One - reactivation of accesses to the Google Drive and Google Classroom for all students.

**Agreed / ~~Not Agreed~~ / ~~Please Discuss~~**

.....  ..... 17/08/2020**Executive Feedback****Background**

1. On 14 August 2020, an email incident occurred across the ACT public school Google platform resulting in the distribution of group emails (including some containing inappropriate material) to students using their Gmail accounts on the Google Suite for Education.
2. The Education Directorate moved quickly to limit user access to the Google Suite for Education (GSFE) including email and the Google platform. Users who remained logged into GSFE had access removed which immediately prevented them from accessing GSFE.
3. The Education Directorate commenced a investigation into the activities causing distribution of material across student cohorts, including inappropriate and explicit content.
4. The Education Directorate has investigated the issue and found:
  - a. The issue originated when a student in Year 6 shared an image as a Google Doc using a Year 8 distribution list.
  - b. The distribution list included Year 8 students from all ACT public schools.
  - c. Sending a request to all year 8 students alerted the cohort that distribution lists are accessible to students.
  - d. The distribution lists were shared with different students in different years and emails went viral.
  - e. Some explicit material was disseminated to students.
  - f. Students emailed this material.

**Issues**

5. The Education Directorate is undertaking a two phased approach to re-establish access to the GSFE for all ACT public school students:
  - a. Phase 1 - Reactivation of accesses to the Google Drive and Google Classroom
  - b. Phase 2 - Reactivation of accesses to Gmail
6. Foresight Consulting was engaged to provide an additional layer of risk assurance across both phases.

Phase One – reactivation of accesses to the Google Drive and Google Classroom

7. Phase one requires that the collaboration settings in Google are reviewed and improved, and that appropriate controls are put in place to ensure the removal of student access to global distribution lists. This will enable the safe reinstatement of Google Drive and Google Classroom access.
8. The Directorate has been working closely with Google and their preferred technical partner, Geeks on Tap, to put the following controls in place:
  - a) Distribution list settings have been changed, meaning that students can no longer see or use Global Groups or Distribution Lists.
  - b) The establishment of additional controls on Administrator access and control, to ensure that future Global Distribution lists cannot be created.
  - c) Students can no longer create groups,
  - d) The autocomplete function for address of email recipients has been deactivated. Students will have to manually enter the address of the individual they wish to send to.
  - e) Arrangements will be in place to actively monitor once the system is back online.
9. These controls have been tested to ensure they are robust and able to be deployed more broadly. The following testing has been conducted:
  - a. Multiple attempts to replicate student activity, including any possible escalations has been completed.
  - b. The Directorate has had multiple parties 'test' the new settings including:
    - a. Education Directorate Staff
    - b. ACT Government SSICT security staff
    - c. Googles preferred technical partner: Geeks on Tap
10. The testing concludes that:
  - a) The settings have successfully copied from the Active Directory to Google
  - b) Gmail will remain deactivated
  - c) Revised settings and controls apply to Google Drive
  - d) Revised settings and controls apply to Google Classroom
  - e) Revised settings and controls apply to Google Meet
  - f) Revised settings and controls apply to Google Doc

11. In summary, three parties have been involved in the testing and cannot recreate the circumstances that led to the initial Email incident.
12. To further support the controls put in place, the Directorate has provided testing logs and scripts to a third part assurer for independent verification.
13. Foresight Consulting has reviewed the response, testing and changes that have been completed and have provided assurance that the controls are adequate. In providing their assurance, Foresight Consulting have made the following comments:

“Foresight have reviewed and assessed ACT Education’s incident management approach in response to the email incident. The containment and recovery of services approach, controls and testing undertaken since the event are considered appropriate for ACT Education’s Phase One plan to re-enable Google for Education services with the exception of Gmail.

Based on our assessment, several areas for improvement exist in the environment that should be considered prior to Phase Two (enabling Gmail service) and for long term management of the environment. Further advice will be provided to support the implementation of Phase Two.”

14. DSST is confident that the issue has been appropriately addressed from a security perspective and this has been independently verified by Foresight Consulting. It is therefore recommended that the Director-General approve the restoration of student access to the Google Drive and Google Classrooms.
15. Following a decision to restore access, real time monitoring by DSST staff will occur for a period of three days, with a possibility of extension. This will further ensure the adequacy of the security controls implemented.
16. Pursuant to agreement of this phase, DSST will initiate planning for phase 2 – reactivation of Gmail.

### **Financial Implications**

17. The Education Directorate has engaged Foresight Consulting to assist at an hourly rate of [REDACTED] (inclusive of GST).

### **Consultation**

#### Internal

18. Service Design and Delivery Group has worked closely with School Improvement Group to manage this incident and communications with schools and families.
19. The Media and Communications and Complaints Handling teams have been informed with respect to the email incident and are providing support with communications to schools, students and their families.

#### Cross Directorate

20. The Education Directorate has worked closely operationally with Shared Services ICT, to ensure that the ICT security measures being taken aligned with WhoG approaches.
21. The Education Directorate notified the ACT Government Chief Digital Officer.

External

22. The Education Directorate notified the Australian Federal Police and Office of the eSafety Commissioner.
23. The Education Directorate has engaged Foresight Consulting to assist with risk and assurance activities.

**Work Health and Safety**

24. Nil.

**Benefits/Sensitivities**

25. Concerns have been raised about the impact on assessment for Year 11 and 12 students due to their GSFE access being removed. Preliminary investigations indicate that the students who disseminated inappropriate material were from this cohort of students.

**Communications, media and engagement implications**

26. The Education Directorate has been working closely with the Minister's Office, media outlets, managing social media and managing communications to the public.
27. The Education Directorate issued letters to parents on Friday 14 August 2020 and 17 August 2020 providing details of the event, the temporary unavailability of the G Suite for Education and the measures being undertaken to provide security assurance.

Signatory Name: Ross Hawkins

Phone:

Action Officer: Kelly Bartlett

Phone:



## Caveat Brief

**To:** Minister for Education and Early Childhood Development  
**From:** Katy Haire, Director-General Education Directorate  
**Subject:** Email incident  
**Date:** 17 August 2020



That you note this update about the email incident which occurred on 14 August 2020, and the activities undertaken to address it

**Noted / Please discuss**

That you note that I have approved an externally assured two phased approach for the reactivation of the Google platform and Gmail for ACT public schools.

**Noted / Please Discuss**

That you endorse my decision to approve reactivation of accesses to the Google Drive and Google Classroom for all students, based on internal and external assurance activities.

**Endorsed / Not Endorsed / Please Discuss**

Yvette Berry MLA 17/08/20

- On 14 August 2020, an email incident occurred across the ACT public school Google platform resulting in the distribution of group emails (including some containing inappropriate material) to students using their Gmail accounts on the Google Suite for Education.
- The Education Directorate limited user access to the Google Suite for Education (GSFE) including email and the Google platform. Users who remained logged into GSFE had access removed which immediately prevented them from accessing GSFE.
- The Education Directorate has investigated the issue and found:
  - a. The issue originated when a student in Year 6 shared an image as a Google Doc using a Year 8 distribution list.
  - b. The distribution list included Year 8 students from all ACT public schools.
  - c. Sending a request to all year 8 students alerted the cohort that distribution lists are accessible to students.

- d. The distribution lists were shared with different students in different years and emails went viral.
- e. Some explicit material was disseminated to students.
- f. Students emailed this material.
- The Education Directorate is approaching the reestablishment of GSFE as a two stage process, to ensure that each element can be security assured:
  - Phase one - Reactivation of accesses to the Google Drive and Classrooms
  - Phase two - Reactivation of accesses to Gmail
- Foresight Consulting was engaged by the Education Directorate to provide an additional layer of risk assurance across both phases.
- Phase one requires that the collaboration settings in Google are reviewed and improved, and that appropriate controls are put in place to ensure the removal of student access to global distribution lists. This will enable the safe reinstatement of Google Drive and Google Classroom access.
- The Directorate has been working closely with Google and their preferred technical partner, Geeks on Tap, to put the following controls in place:
  - Distribution list settings have been changed, meaning that students can no longer see or use Global Groups or Distribution Lists.
  - The establishment of additional controls on Administrator access and control, to ensure that future Global Distribution lists cannot be created.
  - Students can no longer create groups,
  - The autocomplete function for address of email recipients has been deactivated. Students will have to manually enter the address of the individual they wish to send to.
  - Arrangements will be in place to actively monitor once the system is back online.
- These controls have been tested to ensure they are robust and able to be deployed more broadly. The following testing has been conducted:
  - a. Multiple attempts to replicate student activity, including any possible escalations has been completed.
  - b. The Directorate has had multiple parties 'test' the new settings including:
    - a. Education Directorate Staff
    - b. ACT Government SSICT security staff
    - c. Googles preferred technical partner: Geeks on Tap
- The testing concludes that:
  - The settings have successfully copied from the Active Directory to Google
  - Gmail will remain deactivated

- Revised settings and controls apply to Google Drive
- Revised settings and controls apply to Google Classroom
- Revised settings and controls apply to Google Meet
- Revised settings and controls apply to Google Doc
- Three parties have been involved in the testing and cannot recreate the circumstances that led to the initial Email incident.
- To further support the controls put in place, the Directorate has provided testing logs and scripts to a third part assurer for independent verification.
- Foresight Consulting has reviewed the response, testing and changes that have been completed and have provided assurance that the controls are adequate. In providing their assurance, Foresight Consulting have made the following comments:

““Foresight have reviewed and assessed ACT Education’s incident management approach in response to the email incident. The containment and recovery of services approach, controls and testing undertaken since the event are considered appropriate for ACT Education’s Phase One plan to re-enable Google for Education services with the exception of Gmail.

Based on our assessment, several areas for improvement exist in the environment that should be considered prior to Phase Two (enabling Gmail service) and for long term management of the environment. Further advice will be provided to support the implementation of Phase Two.”
- The Education Directorate is confident that the issue has been appropriately addressed from a security perspective and this has been independently verified by Foresight Consulting. It is recommended that restoration of student access to the Google Drive and Google Classrooms is approved, effective immediately.
- Following a decision to restore access, real time monitoring by Education Directorate staff will occur for a period of three days, with a possibility of extension. This will further ensure the adequacy of the security controls implemented.
- The Education Directorate is continuing to work towards Phase Two – reactivation of Gmail.

Signatory Name: Katy Haire  
Title Director-General ACT Education  
Directorate  
Date 17 August 2020

**From:** [Kaur, Puneet](#)  
**To:** [Bartlett, Kelly](#); [McKay, Murray](#)  
**Cc:** [Bayliss, Michael](#)  
**Subject:** RE: FOR APPROVAL: FW: Suspend student's accounts  
**Date:** Tuesday, 18 August 2020 12:32:40 PM  
**Attachments:** [image002.png](#)  
[image004.png](#)  
[image001.jpg](#)

OFFICIAL: Sensitive

Thank you very much [@Bartlett, Kelly](#) and [@McKay, Murray](#)  
 We are proceeding with the below option. Ticket will be raised for this work for future reference.

**Option 2:** MAZE support team change permissions of these students on behalf of schools

Kind Regards

Puneet

---

**From:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
**Sent:** Tuesday, 18 August 2020 12:29 PM  
**To:** McKay, Murray <Murray.McKay@act.gov.au>  
**Cc:** Kaur, Puneet <Puneet.Kaur@act.gov.au>; Bayliss, Michael <Michael.Bayliss@act.gov.au>  
**Subject:** RE: FOR APPROVAL: FW: Suspend student's accounts

OFFICIAL: Sensitive

approved

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 **75663** | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)

---

**From:** McKay, Murray <Murray.McKay@act.gov.au>  
**Sent:** Tuesday, 18 August 2020 11:21 AM  
**To:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
**Cc:** Kaur, Puneet <Puneet.Kaur@act.gov.au>; Bayliss, Michael <Michael.Bayliss@act.gov.au>  
**Subject:** FOR APPROVAL: FW: Suspend student's accounts  
**Importance:** High

OFFICIAL: Sensitive

For approval

**Murray McKay | Director, Digital Literacies**

T: +61 2 620 **59756** | E: [murray.mckay@act.gov.au](mailto:murray.mckay@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#)

---

**From:** Kaur, Puneet <Puneet.Kaur@act.gov.au>  
**Sent:** Tuesday, 18 August 2020 11:19 AM  
**To:** McKay, Murray <Murray.McKay@act.gov.au>; Digital Strategy Services and Transformation <DSST@act.gov.au>  
**Cc:** Bayliss, Michael <Michael.Bayliss@act.gov.au>  
**Subject:** Suspend student's accounts  
**Importance:** High

OFFICIAL

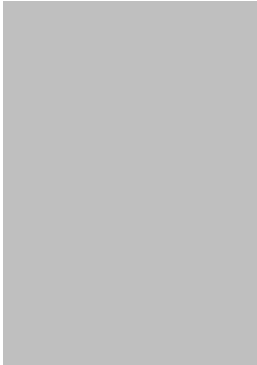
Good Morning,

We received request to suspend below student's accounts as these students are currently suspended by the respective school. To achieve this, ICT Network permission in MAZE needs to be updated to "N" in MAZE. There are two option to achieve this:

**Option 1:** Get schools to modify the permission

**Option 2:** DSST Authorise MAZE support team to change permissions of these students

Please let us know which option best suit you.



Puneet Kaur | Senior Business System Support Officer | Education ICT

**Phone:** +61 2 620 75774 | **Email:** [Puneet.Kaur@act.gov.au](mailto:Puneet.Kaur@act.gov.au)

**Customer Engagement Services Branch | Shared Services ICT | Chief Minister, Treasury and Economic Development Directorate | ACT Government**

51 Fremantle Drive, Stirling, ACT 2611 | GPO Box 158 Canberra ACT 2601 | [www.act.gov.au](http://www.act.gov.au)

*Please consider the environment before printing this email. If printing is necessary, print double-sided and black and white.*





**Portfolio/s:** Education and Early Childhood Development

**ISSUE: EMAIL INCIDENT - 14 AUGUST 2020**

**Key Information:**

- On Friday 14 August 2020, an incident occurred across the ACT Public School Google platform, resulting in the distribution of inappropriate material to of students' Google accounts (including pornography to some accounts).
- The Education Directorate immediately responded to the incident by limiting access to the Google Suite for Education (GSFE), which includes student emails, Google Classrooms, Meets and Docs.
- The Directorate commenced a preliminary investigation into the activities causing the distribution of material across student cohorts.
- There was not an external security breach. No external body hacked the system, nor was any information exported from the system. The system is secure.
- The incident was caused by unintended student access to group distribution email lists.
- A significant number of emails were exchanged, some of which contained inappropriate material, including some pornography.
- Given that some explicit material has been shared, the matter was referred to the AFP and ACT Policing. Notifications were also made to the ACT Chief Digital Office and the eSafety Commissioner.
- A very small number of students were involved in distributing explicit content. The Directorate are taking steps to address this issue with the students and their families directly.
- The Directorate has established a two phase approach to restore Google account access for students:
  - Phase one restored student access to Google Drive and Classroom on 18 August 2020. Prior to restoring accesses, the Directorate conducted rigorous testing on Google Drive and Google Classroom. Assurance was provided by an external consultancy prior to reinstatement of access.
  - Phase two will involve restoring student access to Gmail services and is anticipated by the end of the week. Rigorous testing of

student Gmail services is also being conducted. An external consultancy will provide assurance prior to reactivation of Gmail accounts.

- The Education Directorate will continue to investigate this incident and will ensure that there are appropriate supports for students or their families if they have been adversely impacted.
- Schools have been provided with a learning package to assist with addressing this specific incident in the classroom in an age appropriate manner, as well as eSafety supports for the future.

## **Background**

- Work was completed earlier in the year regarding the creation of background year level groups in Google, that were thought to be inaccessible by students.
- The Directorate immediately began an investigation and engaged an independent consultant to provide oversight of this activity as well as assurance prior to restoration of access to the Google platform.
- The Directorate identified the source of the issue:
  - On 14 August 2020, a student inadvertently shared a file to all students within one of these Groups.
  - Subsequently, some students 'replied all' to this group and began sharing emails. This initial action then escalated to emails being shared across multiple year groups.
- The inappropriate material was first circulated at 12.09 pm and the Education Directorate limited user access to GSFE including email and the Google platform. The system was shut down at 1.00pm. Users who remained logged into GSFE had access removed which immediately prevented them from logging in.
- The Directorate takes the issue of ICT safety and security for their students very seriously. The Directorate have implemented risk control measures prior to restoration of the Google Drive and Google Classroom, assured by an external consultant to provide sufficient risk mitigation prior to restoration of the Google Suite for Education services.
- Testing of Gmail is currently occurring. Appropriate risk controls will be implemented, with assurance provided by an external consultancy prior to access being restored.
- The Directorate has been liaising with the ACT Council of Parents and Citizens Association throughout this process.
- Communications with families regarding the incident were sent on 14 August 2020 and 17 August 2020.
- Schools and the Directorate are continuing to support students adversely impacted by the incident and their families.



From: Bayliss, Michael  
To: Google Cloud Support  
Cc: @google.com; @google.com; @google.com; Will amson, B.I (ACTEDU); Bartlett, KeLy  
Subject: RE: New Case Comment: [#24690438] Exports from Vault stuck at 95%  
Date: Thursday, 20 August 2020 5:37:15 PM  
Attachments: accounts\_with\_matches\_20200820\_0732.csv

---

OFFICIAL

results

-----Original Message-----  
From: Bayliss, Michael <Michael.Bayliss@ed.act.edu.au>  
Sent: Thursday, 20 August 2020 5:29 PM  
To: Bayliss, Michael <Michael.Bayliss@act.gov.au>  
Subject: FW: New Case Comment: [#24690438] Exports from Vault stuck at 95%

---

From: Google Cloud Support  
Sent: Thursday, 20 August 2020 5:28:59 PM (UTC 10:00) Canberra Melbourne Sydney  
To: @google.com; @google.com; Bayliss, Michael; @google.com  
Subject: New Case Comment: [#24690438] Exports from Vault stuck at 95%

Hello,

Google Cloud Support has added a comment to your Support Case #24690438 - Exports from Vault stuck at 95%:

---

Here is the query for Vault search Terms (All Mail Accounts)

-label:\*deleted

With this term, it matches all the undeleted messages across all accounts.

---

Please log into your support portal and post a comment to reply to this update. <https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fenterprise.google.com%2Fsupportcenter%2Fmanagcases%23Case%2F001600000xMmSh%2FU-24690438&campdata=02%7C01%7C%7C5bdcd719f1f244d6b6f308d844dac642%7Cb46c190803344236b978585ee88e4199%7C0%7C1%7C63733505369748094&campdata=j6qWWUHXMImN5RdwGwL2bMsAL46sstF3Cb4VzzZTM%3D&campreserved=0>  
The owner of your case will be notified of any updates you make.

You can also respond directly to this email. However, your email response will not show in your Google Cloud Support Center (GCSC).

Regards,

Google Cloud Support

[ref:\_00D00VwG\_5005w1cN6oqref]

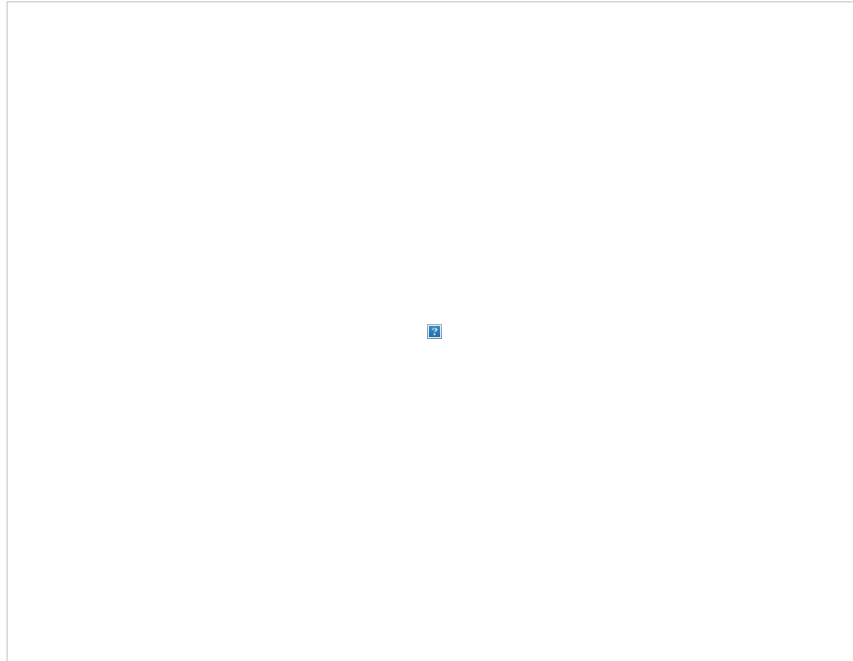
The attachment is not released in accordance with section 17 of the *Freedom of Information Act 2016* - Schedule 2, 2.2(a)(ii)

**From:** Bayliss, Michael  
**To:** Crawford, Jodie; Digital Strategy Services and Transformation  
**Cc:** Bartlett, Kelly; Williamson, Bill (ACTEDU); Sanderson, Mark; Ruecroft, Daniel; Kaur, Puneet; Malhotra, Vish; Al Mamun, Md Abdulah  
**Subject:** RE: G Suite status alert  
**Date:** Friday, 21 August 2020 9:14:39 AM  
**Attachments:** [image005.png](#)  
[image006.png](#)  
[image007.png](#)  
[image008.png](#)  
[image009.png](#)

OFFICIAL

Update -

The Google service disruptions were all reported as resolved overnight.



**From:** Bayliss, Michael

**Sent:** Thursday, 20 August 2020 6:27 PM

**To:** Crawford, Jodie <Jodie.Crawford@act.gov.au>; Digital Strategy Services and Transformation <DSST@act.gov.au>

**Cc:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>; Williamson, Bill (ACTEDU) <Bill.Williamson@ed.act.edu.au>; Sanderson, Mark <Mark.Sanderson@act.gov.au>; Ruecroft, Daniel <Daniel.Ruecroft@act.gov.au>

**Subject:** RE: G Suite status alert

OFFICIAL

Update -

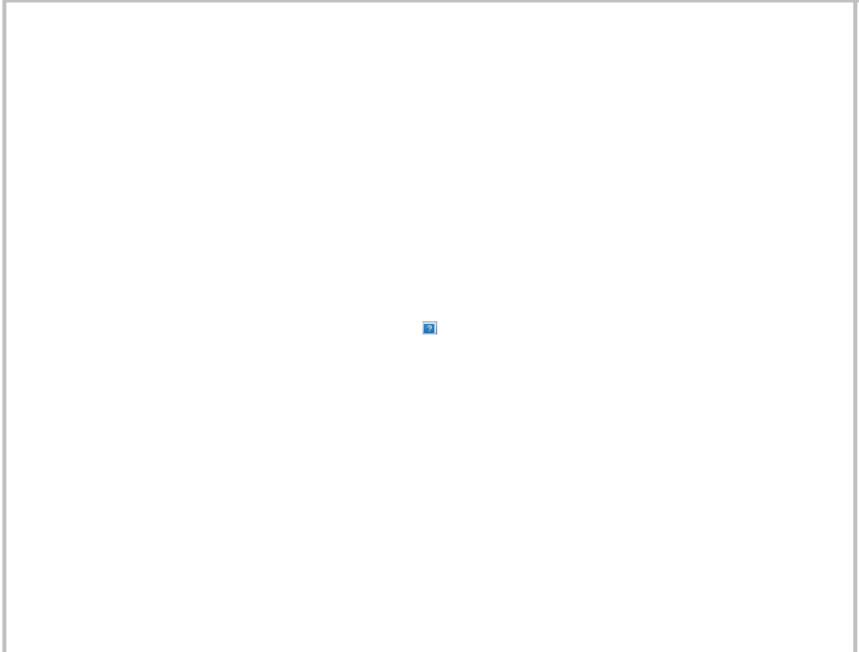
Google has posted an update on the service disruption -

Our team is continuing to investigate this issue. We will provide an update by 20/08/2020 18:21 with more information about this problem. Thank you for your patience.

- Gmail sending issues,
- Meet recording issues,
- Creating files issues in Drive,
- CSV user upload issues in Admin Console,
- Posting message issues in Google Chat

More services have also been highlighted as affected.

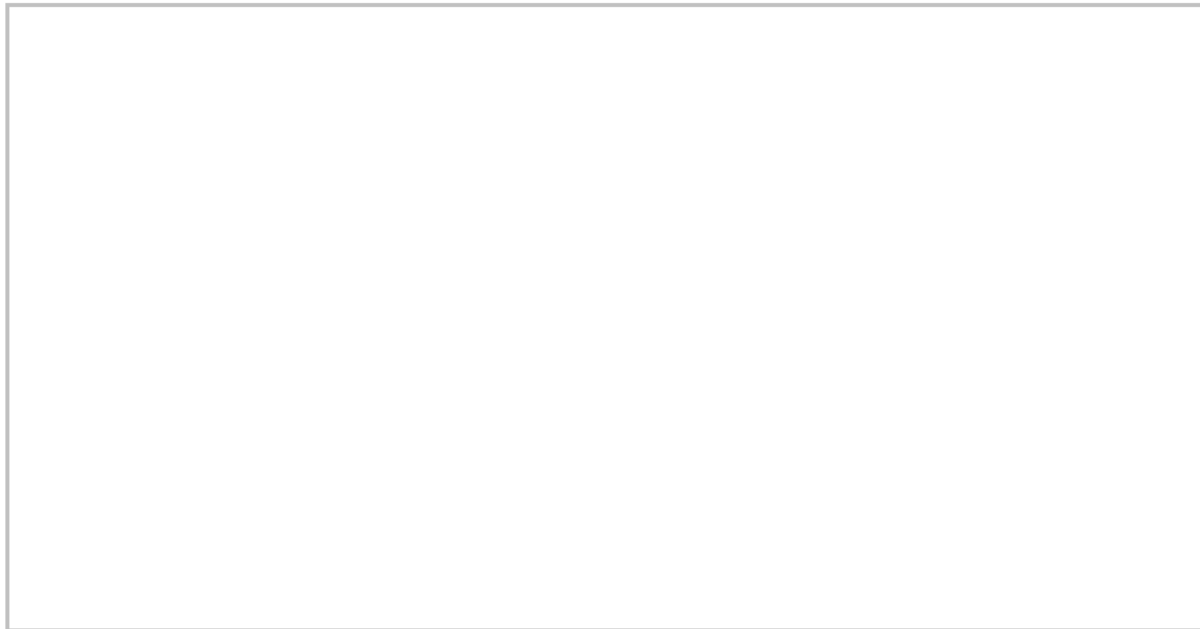
- Gmail
- Google Drive
- Google Docs
- Google Groups
- Google Chat
- Google Meet
- Google Keep
- Google Voice



**From:** Bayliss Michael  
**Sent:** Thursday 20 August 2020 4 26 PM  
**To:** Crawford Jodie <[Jodie.Crawford@act.gov.au](mailto:Jodie.Crawford@act.gov.au)>; Digital Strategy Services and Transformation <[DSST@act.gov.au](mailto:DSST@act.gov.au)>  
**Cc:** Bartlett Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>; Williamson Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; Sanderson Mark <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>; Ruecroft Daniel <[Daniel.Ruecroft@act.gov.au](mailto:Daniel.Ruecroft@act.gov.au)>  
**Subject:** RE: G Suite status alert

OFFICIAL

Update –  
I've done a quick test of each of the services (excluding Gmail) and they appear to be working normally for me. So this service disruption **may not actually be impacting ACT Education users in a noticeable way**. Each of the cases contain the same information - they are investigating and will have an update at 6pm tonight.



Cheers

Michael

From: Bayliss Michael

Sent: Thursday 20 August 2020 4 16 PM

To: Crawford Jodie <[Jodie.Crawford@act.gov.au](mailto:Jodie.Crawford@act.gov.au)>; Digital Strategy Services and Transformation <[DSST@act.gov.au](mailto:DSST@act.gov.au)>

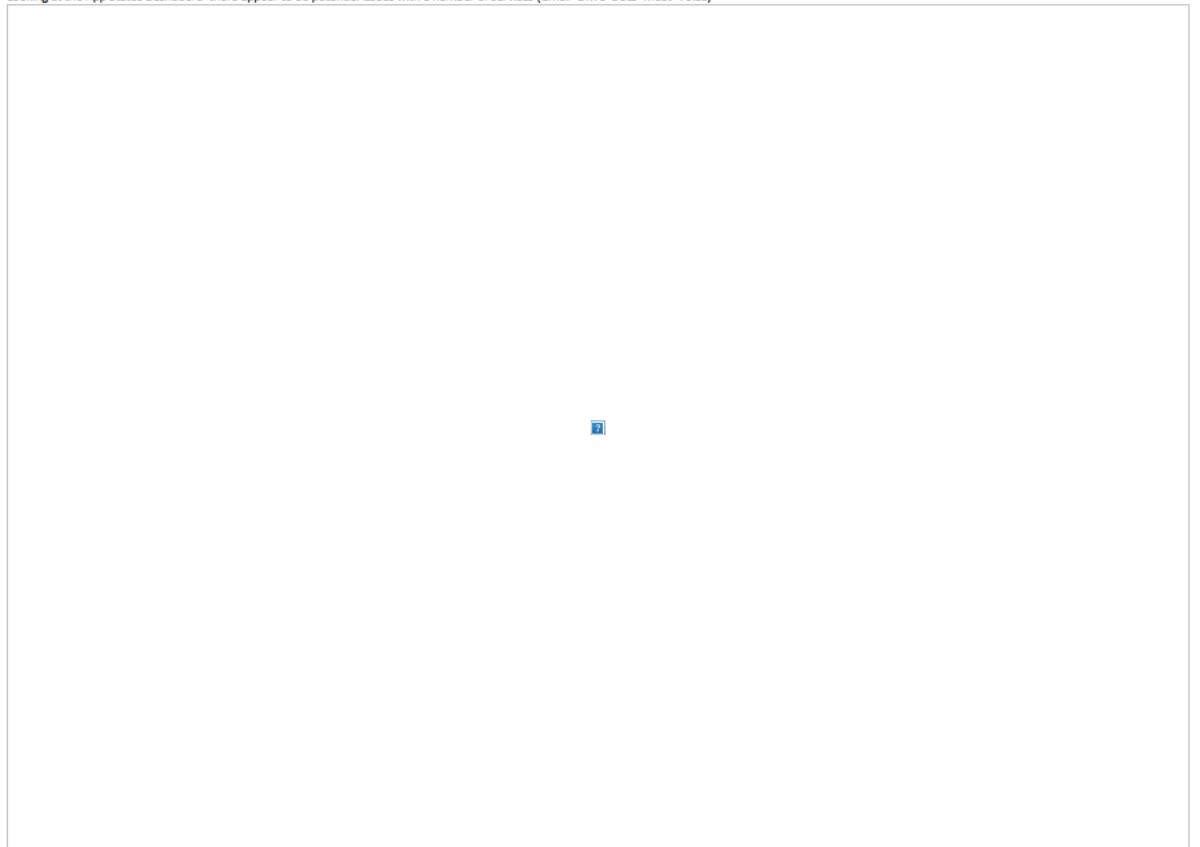
Cc: Bartlett Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>; Williamson Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; Sanderson Mark <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>; Ruecroft Daniel <[Daniel.Ruecroft@act.gov.au](mailto:Daniel.Ruecroft@act.gov.au)>

Subject: FW: G Suite status alert

OFFICIAL

FYI – Google has reported a potential service disruption to Drive.

Looking at the App Status Dashboard there appear to be potential issues with a number of services (Gmail Drive Docs Meet Voice)



From: Bayliss Michael <[Michael.Bayliss@ed.act.edu.au](mailto:Michael.Bayliss@ed.act.edu.au)>

Sent: Thursday 20 August 2020 4 11 PM

To: Bayliss Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>

Subject: FW: G Suite status alert

From: The G Suite Team

Sent: Thursday, 20 August 2020 4:10:38 PM (UTC+10:00) Canberra, Melbourne, Sydney

To: Bayliss, Michael

Subject: G Suite status alert



Status: [Service disruption](#)

August 19, 2020 10:29:00 PM PDT

We're investigating reports of an issue with Google Drive. We will provide more information shortly.

[Learn more about G Suite administrator email alerts.](#)

Sincerely,

The G Suite Team



© 2020 Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043

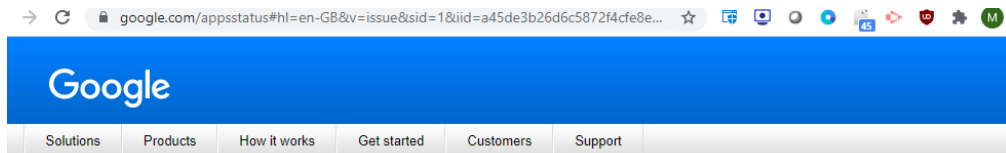
You have received this important update about your G Suite account because you designated this email address as a primary or secondary contact for mandatory service communications in your Google [Admin console](#) profile.

Image 005

Current status	15/08/2020	16/08/2020	17/08/2020	18/08/2020	19/08/2020	20/08/2020	21/08/2020
Gmail							
Google Calendar							
Google Drive							
Google Docs							
Google Sheets							
Google Slides							
Google Sites							
Google Groups							
Google Hangouts							
Google Chat							
Google Meet							
Google Vault							
Currents							
Google Forms							
Google Cloud Search							
Google Keep							
Google Tasks							
Google Voice							

[« Older](#) [Newer »](#)

Image 006



## Gmail - Service Details

[G Suite Status Dashboard](#)

This page offers performance information for the following Google services. Unless otherwise noted, this status information applies to consumer services as well as services for organizations using G Suite.

Check back here any time to view the current status of the services listed below. For additional information or to report a problem, please visit the [G Suite Help Center](#) or see the [G Suite Known Issues](#) page.

Time:	Description
20/08/2020 17:21	Our team is continuing to investigate this issue. We will provide an update by 20/08/2020 18:21 with more information about this problem. Thank you for your patience.  Gmail sending issues, Meet recording issues, Creating files issues in Drive, CSV user upload issues in Admin Console, Posting message issues in Google Chat
20/08/2020 17:09	We are continuing to investigate this issue. We will provide an update by 20/08/2020 18:09 detailing when we expect to resolve the problem.
20/08/2020 17:04	We are continuing to investigate this issue. We will provide an update by 20/08/2020 18:04 detailing when we expect to resolve the problem.
20/08/2020 16:07	We are continuing to investigate this issue. We will provide an update by 20/08/2020 18:00 detailing when we expect to resolve the problem.
20/08/2020 15:29	We're investigating reports of an issue with Gmail. We will provide more information shortly.

All times are shown in your local time zone unless otherwise noted.

[RSS Feed](#)

No Issues   Service disruption   Service outage


Image 007

Current status	14/08/2020	15/08/2020	16/08/2020	17/08/2020	18/08/2020	19/08/2020	20/08/2020
● Gmail							●
● Google Calendar							
● Google Drive							●
● Google Docs							●
● Google Sheets							
● Google Slides							
● Google Sites							
● Google Groups							●
● Google Hangouts							
● Google Chat							●
● Google Meet							●
● Google Vault							
● Currents							
● Google Forms							
● Google Cloud Search							
● Google Keep							●
● Google Tasks							
● Google Voice							●

« Older   Newer »

Image 008

google.com/appsstatus#hl=en-GB&v=issue&sid=18&iid=a45de3b26d6c5872f4cfe8e3424d7a82



[Solutions](#)   [Products](#)   [How it works](#)   [Get started](#)   [Customers](#)   [Support](#)

## Gmail - Service Details

G Suite Status Dashboard

This page offers performance information for the following Google services. Unless otherwise noted, this status information applies to consumer services as well as services for organizations using G Suite.

Check back here any time to view the current status of the services listed below. For additional information or to report a problem, please visit the [G Suite Help Center](#) or see the [G Suite Known Issues](#) page.

Time:	Description
● 20/08/2020 16:07	We are continuing to investigate this issue. We will provide an update by 20/08/2020 18:00 detailing when we expect to resolve the problem.
● 20/08/2020 15:29	We're investigating reports of an issue with Gmail. We will provide more information shortly.

All times are shown in your local time zone unless otherwise noted. [RSS Feed](#)

● No Issues   
 ● Service disruption   
 ● Service outage

---

[Google Home](#) - [Privacy](#) - [About Google](#) - [Support](#)  
 ©2020 Google - Last updated: 20 August 2020 16:11:31 UTC+10



Image 009

google.com/appsstatus#hl=en-GB&v=status

This page offers performance information for the following Google services. Unless otherwise noted, this status information applies to consumer services as well as services for organizations using G Suite.

Check back here any time to view the current status of the services listed below. For additional information or to report a problem, please visit the [G Suite Help Center](#) or see the [G Suite Known Issues](#) page.

Products covered by [G Suite Service Level Agreement](#) and [Technical Support Service Guidelines](#):

Current status	14/08/2020	15/08/2020	16/08/2020	17/08/2020	18/08/2020	19/08/2020	20/08/2020
Gmail							
Google Calendar							
Google Drive							
Google Docs							
Google Sheets							
Google Slides							
Google Sites							
Google Groups							
Google Hangouts							
Google Chat							
Google Meet							
Google Vault							
Currents							
Google Forms							
Google Cloud Search							
Google Keep							
Google Tasks							
Google Voice							

[« Older](#) [Newer »](#)

Products covered by [G Suite Service Level Agreement](#), [Cloud Identity Service Level Agreement](#) and [Technical Support Service Guidelines](#):

**From:** [REDACTED]@google.com>

**Sent:** Friday, 21 August 2020 4:34 PM

**To:** McKay, Murray <Murray.McKay@act.gov.au>

**Cc:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>; [REDACTED]@google.com>; Bayliss, Michael <Michael.Bayliss@act.gov.au>; Williamson, Bill (ACTEDU) <Bill.Williamson@ed.act.edu.au>

**Subject:** Re: Purge Job

**CAUTION:** This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hi Murray,

Yes, you should probably disable it for Drive.

You might want to check the "[default link sharing](#)" setting as well.

Cheers,

[REDACTED]

On Fri, Aug 21, 2020 at 2:24 PM McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)> wrote:

OFFICIAL

Hi all

My questions for this afternoon:

- We noticed that the move to Enterprise turned on some cloud search functionality that we might not have been aware of and this has resulted in reports of students being able to see files not intended for their access when searching their drive. We understand that these files were probably always accessible to students, but the cloud search functionality is making them far more visible. I turned the following setting off in the console, but am interested to know if there are other Enterprise settings that may need adjustment in light of the week we have had.

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the navigation path is: Apps > G Suite > Settings for Drive and Docs > Features and Applications. The main content area is divided into two columns. The left column is a sidebar for 'Drive and Docs' with options for Users, Groups, and Organisational units. The right column shows settings for 'Add-Ons' and 'Surface suggestions in Google Chrome'. The 'Add-Ons' setting is 'ON'. The 'Surface suggestions in Google Chrome' setting is currently set to 'Allow Google Drive file suggestion performed (recommended)'. A red circle highlights this setting, and a red line connects it to the 'Add-Ons' setting. Below the 'Surface suggestions in Google Chrome' setting, there is an information icon and a note: 'Changes may take up to 24 hours to propagate. Prior changes can be seen in [Audit log](#)'.

Another technical question I have is how we can configure email recipient limits for students (to less than 30). I tried this, but it is not working yet:

## Murray McKay | Director, Digital Literacies

T: +61 2 620 59756 | E: [murray.mckay@act.gov.au](mailto:murray.mckay@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#)

**From:** McKay, Murray

**Sent:** Friday, 21 August 2020 9:17 AM

**To:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>; [\[REDACTED\]@google.com](mailto: [REDACTED]@google.com)>

**Cc:** [\[REDACTED\]@google.com](mailto: [REDACTED]@google.com)>; Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>

**Subject:** RE: Purge Job

## OFFICIAL

Thanks - I haven't had much luck on the support line this morning:

This is an automated email from Google Cloud Support. Case #24773999 has been created or updated. Here are some details about your case:

---

**Status:** Assigned

**Subject:** Would like a status report for case #24690438

**Description:**

Chat Started: Thu, 20 Aug 2020 17:38:27 -0500 Chat Subject: Would like a status report for case #24690438 G Suite Support, [REDACTED]: Thank you for contacting G Suite Support. My name is [REDACTED] and I'll be working with you today. While I read over your message, is there anything else you'd like to add? G Suite Support, [REDACTED]: Sure, give me 2 minutes to check the case Murray McKay: No - just need an update as to the status of our gmail purge process G Suite Support, [REDACTED]: Sure G Suite Support, [REDACTED]: Last updated was sent today and you replied, after your last reply there's no more G Suite Support, [REDACTED]: I place a note to the agent to contact you, as this is already being handled by a Tier 2 Murray McKay: That was 15 hours ago. An upgrade from the would be very helpful G Suite Support, [REDACTED]: I just notified the agent so he will contact you if there's something new about it G Suite Support, [REDACTED] can you confirm your phone number Murray McKay: I would really like an update either way - Murray McKay: [REDACTED] G Suite Support, [REDACTED]: You mean, an update from me? Murray McKay: no from the tier 2 contact G Suite Support, [REDACTED] Oh, yes I just placed the note to notify the agent and send you an email with the update G Suite Support, [REDACTED]: So please keep an eye in your inbox Murray McKay: thank you G Suite Support, [REDACTED]: Sorry for the delays G Suite Support, [REDACTED]: For now is there anything else I can help you with? Murray McKay: no thats it. thanks G Suite Support, [REDACTED]: Thanks for chatting with Google Cloud Support! Keep in mind that you have 30 days to reopen this case if further assistance is needed.

---

**Google Cloud Support**

<https://support.google.com/googlecloud/apps/>

**Murray McKay | Director, Digital Literacies**

T: +61 2 620 59756 | E: [murray.mckay@act.gov.au](mailto:murray.mckay@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#)

[REDACTED]

---

**From:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>  
**Sent:** Friday, 21 August 2020 9:16 AM  
**To:** [REDACTED] <[\[REDACTED\]@google.com](mailto:[REDACTED]@google.com)>  
**Cc:** [REDACTED] <[\[REDACTED\]@google.com](mailto:[REDACTED]@google.com)>; Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>  
**Subject:** RE: Purge Job

OFFICIAL

Thank you

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)

[REDACTED]

---

**From:** [REDACTED] <[\[REDACTED\]@google.com](mailto:[REDACTED]@google.com)>  
**Sent:** Friday, 21 August 2020 9:14 AM  
**To:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>  
**Cc:** [REDACTED] <[\[REDACTED\]@google.com](mailto:[REDACTED]@google.com)>; Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>  
**Subject:** Re: Purge Job

**CAUTION:** This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hi Kelly,

[REDACTED] is looking into the case as we speak... will report back shortly.

Best,

[REDACTED]

On Fri, Aug 21, 2020 at 8:46 AM Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)> wrote:

OFFICIAL

Hi Everyone

Have we heard anything from the USA team- ideally if we can have an email update this morning and then discuss at 10:30am

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: [0422 233 772](tel:0422 233 772) | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)

[REDACTED]

-----  
This email, and any attachments, may be confidential and also privileged. If you are not the intended recipient,

please notify the sender and delete all copies of this transmission along with any attachments immediately. You should not copy or use it for any purpose, nor disclose its contents to any other person.

-----

--



Google for Education



|



**From:** [Williamson, Bill](#)  
**To:** [Valtas, Julian](#); [Ruecroft, Daniel](#); [Sanderson, Mark](#); [Bayliss, Michael](#)  
**Cc:** [Bartlett, Kelly](#); [McKay, Murray](#)  
**Subject:** Creating OUs and enabling gmail -- limited users  
**Date:** Monday, 24 August 2020 9:15:38 AM  
**Attachments:** [image001.png](#)

---

Hi All,

For the following users I am doing these steps:

- Look up user
- Create a subOU called "GMAIL\_TEST" under their substantive OU
- Turning Gmail on for that OU
- Moving the student into that OU
- Delegating the user's mailbox to myself/Kelly/murray (via script)
- Checking mailbox for "odd" messages that aren't showing up properly in the backend (mostly chats we've discovered)
- Screenshot/noting results
- Reverting the above steps



**Bill Williamson | Senior Director - School Administration System Architecture**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

[cid:image002.png@01D4E953.9786AC90](#)

**From:** [Google Cloud Support](#)  
**To:** [Bartlett, Kelly](#); [Williamson, Bill \(ACTEDU\)](#)  
**Cc:** [@google.com](#); [Sanderson, Mark](#); [McKay, Murray](#); [Bayliss, Michael](#)  
**Subject:** RE: Delete progress [#24690438] -- URGENT [ ref:\_00D00VNwG.\_5005w1cN6oq:ref ]  
**Date:** Monday, 24 August 2020 3:48:39 PM

---

CAUTION: This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hi Kelly,

Thank you for the confirmation. I will let the team know and pause the rollout process for the script.

Thanks.

----- Original Message -----

**From:** Bartlett, Kelly [kelly.bartlett@act.gov.au]  
**Sent:** 8/24/2020 3:25 PM  
**To:** [@google.com](#); [bill.williamson@ed.act.edu.au](#)  
**Cc:** [murray.mckay@act.gov.au](#); [@google.com](#); [michael.bayliss@act.gov.au](#); [mark.sanderson@act.gov.au](#)  
**Subject:** RE: Delete progress [#24690438] -- URGENT [ ]

OFFICIAL

Hi [@google.com](#)

I can confirm that the script from the Google Engineering team is no longer required.

Regards,

Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)  
T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)  
Digital Strategy, Services & Transformation | Education | ACT Government  
51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
<http://www.education.act.gov.au/>

-----Original Message-----

**From:** Google Cloud Support [@google.com](#)>  
**Sent:** Monday, 24 August 2020 2:22 PM  
**To:** Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>  
**Cc:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>; [@google.com](#); Sanderson, Mark <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>; McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>  
**Subject:** RE: Delete progress [#24690438] -- URGENT [ ]

CAUTION: This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Thanks for the update. It's glad to hear that the message purging job is completed!

It seems the message purging script from Gmail engineering team is no longer required. Can you confirm that so I can let the team know ?

Thanks.  
[REDACTED]

----- Original Message -----

From: Williamson, Bill [bill.williamson@ed.act.edu.au]  
Sent: 8/24/2020 2:00 PM  
To: [REDACTED]@google.com  
Cc: kelly.bartlett@act.gov.au; murray mckay@act.gov.au; [REDACTED]@google.com; michael.bayliss@act.gov.au; mark.sanderson@act.gov.au  
Subject: RE: Delete progress [#24690438] -- URGENT [ ]

We have completed the purge.

We have discovered that these "ghost" messages are hangouts chats that live in a user's inbox, but aren't real emails, hence no message ID etc.

Bill Williamson | Senior Director  
T: 0430 333 647 | E: bill.williamson@ed.act.edu.au Digital Strategy, Services & Transformation | Education | ACT Government  
51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601 <http://www.education.act.gov.au/> | Facebook | Twitter | Instagram | LinkedIn | Google+

-----Original Message-----

From: Google Cloud Support [REDACTED]@google.com>  
Sent: Monday, 24 August 2020 1:59 PM  
To: Williamson, Bill <Bill.Williamson@ed.act.edu.au>  
Cc: Bartlett, Kelly (ACTGOV) <Kelly.Bartlett@act.gov.au>; [REDACTED]@google.com; Sanderson, Mark (ACTGOV) <Mark.Sanderson@act.gov.au>; McKay, Murray (ACTGOV) <Murray.McKay@act.gov.au>; Bayliss, Michael (ACTGOV) <Michael.Bayliss@act.gov.au>  
Subject: Re: Delete progress [#24690438] -- URGENT [ ]

Hi Bill,

Just wanted to followup on this one. How's the purging job going ?

Thanks.  
[REDACTED]

----- Original Message -----

From: [REDACTED]@google.com]  
Sent: 8/22/2020 5:01 PM  
To: bill.williamson@ed.act.edu.au  
Cc: kelly.bartlett@act.gov.au; [REDACTED]@google.com; murray.mckay@act.gov.au; [REDACTED]@google.com; michael.bayliss@act.gov.au; mark.sanderson@act.gov.au  
Subject: Re: Delete progress [#24690438] [ ] -- URGENT

Hi Bill,

It looks like the job can't query the message by internal ID with your query, and that's why it can't display the MessageID and Subject.

Can you run some searches by checking some accounts in the list ? Either in the investigation tool or Vault (with terms: -label:^deleted) ?

Cheers,  
[REDACTED]


On Sat, Aug 22, 2020 at 4:38 PM Williamson, Bill <Bill.Williamson@ed.act.edu.au> wrote:

> Hi all,  
 >  
 >  
 >  
 > We keep running into really odd errors where there are no subject in a  
 > message, and it then errors out when deleting them. Our worry is that  
 > they might represent a real message in a mailbox, but we have no way to verify.  
 >  
 >  
 >  
 >  
 >  
 >  
 >  
 >  
 > \*Bill Williamson | Senior Director - School Administration System  
 > Architecture\*  
 >  
 > T: 0430 333 647 | E: bill.williamson@ed.act.edu.au  
 >  
 > Digital Strategy, Services & Transformation | Education | ACT  
 > Government  
 >  
 > 51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
 >  
 > <http://www.education.act.gov.au/> | Facebook  
 > <<https://aus01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.facebook.com%2Fpages%2FACT-Public-Schools%2F94038489456%3Fref%3Dts&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&sdata=li4NsJ8ZMZxVHN%2BnSz5wCigFCzqKuQJEyxb1QqnbL9Y%3D&reserved=0>>  
 > | Twitter  
 > <<https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FACTEducation&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&sdata=xa7pNyib7TU41vpyl6l0d2QueenmoV%2FCiVkbCTjv%2BjVA%3D&reserved=0>> | Instagram  
 > <<https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.instagram.com%2Factpublicschools%2F&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&sdata=8pAmQ8fYcff1Jcb4Nka%2FHjtXiS0FBdARy2NX4b1%2BzFc%3D&reserved=0>> | LinkedIn  
 > <<https://aus01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.linkedin.com%2Fcompany%2F706896%3Ftrk%3Dtyah&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&sdata=LyivNrQ2%2BblzIt4krWtV3IU8ULYrOq4YbSu83tK9I34%3D&reserved=0>> | Google+  
 > <<https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fplus.google.com%2F103779771541941617837%2Fposts%2310377977154194161&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&sdata=wwet7XZkJa%2BIckqamJ1bho3wzqdNq5x7hJHZIVtRoZU%3D&reserved=0>>  
 > 7837/posts>  
 >  
 >  
 >  
 > [image: cid:image002.png@01D4E953.9786AC90]  
 >  
 >  
 >

> \*From:\* [REDACTED]@google.com>  
 > \*Sent:\* Friday, 21 August 2020 7:30 PM  
 > \*To:\* Bayliss, Michael (ACTGOV) <Michael.Bayliss@act.gov.au>  
 > \*Cc:\* Bartlett, Kelly (ACTGOV) <Kelly.Bartlett@act.gov.au>; [REDACTED]  
 > [REDACTED]@google.com>; Williamson, Bill  
 > <Bill.Williamson@ed.act.edu.au>; Google Cloud Support  
 > [REDACTED]@google.com>; McKay, Murray (ACTGOV) <  
 > Murray.McKay@act.gov.au>; Sanderson, Mark (ACTGOV) <  
 > Mark.Sanderson@act.gov.au>  
 > \*Subject:\* Re: Delete progress [#24690438] [ ]  
 >  
 >  
 >  
 > Thanks for the update - hopefully it continues chugging along. Please  
 > keep us posted!  
 >  
 > On Fri, 21 Aug 2020, 4:43 pm Bayliss, Michael,  
 > <Michael.Bayliss@act.gov.au>  
 > wrote:  
 >  
 > OFFICIAL  
 >  
 >  
 >  
 > Update –  
 >  
 >  
 >  
 > Now less than 7.6M emails remaining. Deletion looks to have sped up  
 > somewhat through the day, last few hours measuring around [REDACTED] deletes  
 > per hour. Current ETA looking around Saturday [REDACTED].  
 >  
 >  
 >  
 > Updated spreadsheet attached, has been tidied up somewhat as well.  
 >  
 >  
 >  
 >  
 >  
 >  
 > \*From:\* Bayliss, Michael  
 > \*Sent:\* Friday, 21 August 2020 1:38 PM  
 > \*To:\* Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
 > \*Cc:\* [REDACTED]@google.com>; Williamson, Bill (ACTEDU) <  
 > Bill.Williamson@ed.act.edu.au>; [REDACTED]@google.com>;  
 > Google Cloud Support [REDACTED]@google.com>; McKay, Murray <  
 > Murray.McKay@act.gov.au>  
 > \*Subject:\* RE: Delete progress [#24690438] [ ]  
 >  
 >  
 >  
 > OFFICIAL  
 >  
 >  
 >  
 > Update –  
 >  
 >  
 >  
 > Currently at about 8.6M emails remaining to be deleted.  
 >



> Murray.McKay@act.gov.au>  
> \*Subject:\* RE: Delete progress [#24690438] [ ]  
>  
>  
>  
> OFFICIAL  
>  
>  
>  
> Hi Kelly,  
>  
>  
>  
> Update –  
>  
>  
>  
> Deletion progress below, apologies it's a bit ugly atm, trying to get  
> it into an easy to follow graph.  
>  
>  
>  
> Latest count was around 9.4M not deleted, or 56.61% not deleted.  
>  
>  
>  
> Based on current deletion rates, looking like ~[REDACTED] hours ETA.  
>  
>  
>  
>  
> Export  
>  
> Query Date  
>  
> Minutes  
>  
> Total count  
>  
> Not deleted Count  
>  
> Not Deleted %  
>  
> Delta T (mins)  
>  
> Delta Count  
>  
> Deletes per minute  
>  
> Deletes per hour  
>  
> Deletes per 24 hours  
>  
> Eta (hours)  
>  
> ?  
>  
> 9774910  
>  
> accounts\_with\_matches\_20200821\_0009.csv

>  
> 2020-08-21T00:09:12.562Z  
>  
> 9  
>  
> 16600180  
>  
> 9582687  
>  
> 57.73%  
>  
> ?  
>  
> 192223  
>  
> #VALUE!  
>  
> #VALUE!  
>  
> #VALUE!  
>  
> #VALUE!  
>  
> accounts\_with\_matches\_20200821\_0025.csv  
>  
> 2020-08-21T00:25:48.548Z  
>  
> 25  
>  
> 16600180  
>  
> 9519721  
>  
> 57.35%  
>  
> 16  
>  
>   
>  
> accounts\_with\_matches\_20200821\_0035.csv  
>  
> 2020-08-21T00:35:11.984Z  
>  
> 35  
>  
> 16600180  
>  
> 9482467  
>  
> 57.12%  
>  
> 10  
>



> [REDACTED]  
> [REDACTED]  
> [REDACTED]  
> [REDACTED]  
> [REDACTED]

>  
> accounts\_with\_matches\_20200821\_0051.csv

>  
> 2020-08-21T00:51:28.849Z

>  
> 51

>  
> 16600180

>  
> 9397619

>  
> 56.61%

>  
> 16

> [REDACTED]  
> [REDACTED]  
> [REDACTED]  
> [REDACTED]  
> [REDACTED]

>  
>  
>  
>  
>  
>  
> \*From:\* Bayliss, Michael  
> \*Sent:\* Friday, 21 August 2020 10:01 AM  
> \*To:\* Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
> \*Cc:\* [REDACTED]@google.com>; Williamson, Bill (ACTEDU) <Bill.Williamson@ed.act.edu.au>; [REDACTED]@google.com>;  
> Google Cloud Support [REDACTED]@google.com>; McKay, Murray <Murray.McKay@act.gov.au>  
> \*Subject:\* RE: Delete progress [#24690438] [ ]

>  
>  
>  
>  
> OFFICIAL

>  
>  
>  
>  
> Yep no worries Kelly.

>  
>  
>  
>  
> \*From:\* Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
> \*Sent:\* Friday, 21 August 2020 10:00 AM  
> \*To:\* Bayliss, Michael <Michael.Bayliss@act.gov.au>  
> \*Cc:\* [REDACTED]@google.com>; Williamson, Bill (ACTEDU) <

> Bill.Williamson@ed.act.edu.au>; [REDACTED]@google.com>;  
> Google Cloud Support [REDACTED]@google.com>; McKay, Murray <  
> Murray.McKay@act.gov.au>  
> \*Subject:\* RE: Delete progress [#24690438] [ ]  
>  
>  
>  
> OFFICIAL  
>  
>  
>  
> Hi Michael  
>  
>  
>  
> Given the several jobs we setup seems to be progressing. Can you  
> please provide me with an updated report at 11am?  
>  
>  
>  
> The jobs seems to be working from Murray's account but not Bill's.  
>  
>  
>  
> Regards,  
>  
>  
>  
> \*Kelly Bartlett | A/G Executive Branch Manager (Chief Information  
> Officer)\*  
>  
> T: +61 2 620 \*75663\* | M: 0422 233 772 | E: kelly.bartlett@act.gov.au  
>  
> Digital Strategy, Services & Transformation | Education | ACT  
> Government  
>  
> 51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
>  
> <http://www.education.act.gov.au/>  
>  
>  
>  
>  
>  
>  
>  
> \*From:\* Bayliss, Michael <Michael.Bayliss@act.gov.au>  
> \*Sent:\* Friday, 21 August 2020 9:36 AM  
> \*To:\* McKay, Murray <Murray.McKay@act.gov.au>; Bartlett, Kelly <  
> Kelly.Bartlett@act.gov.au>; [REDACTED]@google.com>; Google  
> Cloud Support [REDACTED]@google.com>  
> \*Cc:\* [REDACTED]@google.com>; Williamson, Bill (ACTEDU) <  
> Bill.Williamson@ed.act.edu.au>  
> \*Subject:\* Delete progress [#24690438] [ ]  
>  
>  
>  
> OFFICIAL  
>  
>  
>  
> Hi All,  
>

>  
>  
> I have re-run the delete label counts as explained yesterday by [REDACTED],  
> and it looks like the deletion has moved along significantly  
> overnight. The queries counted are screenshotted below.  
>  
>  
>  
> Overall it looks like 6.8M deleted, with another ~9.7M not yet deleted.  
>  
>  
>  
> total  
>  
> approx  
> 16600180  
>  
> not deleted  
>  
> approx  
>  
> 9774910  
>  
> 59%  
>  
> deleted  
>  
> approx  
>  
> 6825270  
>  
> 41%  
>  
>  
>  
>  
>  
> Not deleted count:  
>  
>  
>  
> Total count:  
>  
>  
>  
>  
>  
>  
>  
>  
>  
>  
> \*From:\* McKay, Murray <Murray.McKay@act.gov.au>  
> \*Sent:\* Friday, 21 August 2020 9:17 AM  
> \*To:\* Bartlett, Kelly <Kelly.Bartlett@act.gov.au>; [REDACTED]  
> [REDACTED]@google.com>  
> \*Cc:\* [REDACTED]@google.com>; Bayliss, Michael <  
> Michael.Bayliss@act.gov.au>; Williamson, Bill (ACTEDU) <  
> Bill.Williamson@ed.act.edu.au>  
> \*Subject:\* RE: Purge Job  
>

>  
>  
> OFFICIAL  
>  
>  
>  
> Thanks - I haven't had much luck on the support line this morning:  
>  
>  
>  
> This is an automated email from Google Cloud Support. Case #24773999  
> has been created or updated. Here are some details about your case:  
> -----  
>  
> \*Status:\* Assigned  
> \*Subject:\* Would like a status report for case #24690438  
> \*Description:\*  
> Chat Started: Thu, 20 Aug 2020 17:38:27 -0500 Chat Subject: Would like  
> a status report for case #24690438 G Suite Support, [REDACTED]: Thank you  
> for contacting G Suite Support. My name is [REDACTED] and I'll be working  
> with you today. While I read over your message, is there anything else  
> you'd like to add? G Suite Support, [REDACTED]: Sure, give me 2 minutes to  
> check the case Murray McKay: No - just need an update as to the status  
> of our gmail purge process G Suite Support, [REDACTED]: Sure G Suite  
> Support, [REDACTED] Last updated was sent today and you replied, after  
> your last reply there's no more G Suite Support, [REDACTED]: I place a  
> note to the agent to contact you, as this is already being handled by a Tier 2 Murray McKay: That was 15  
> hours ago.  
> An upgrade from the would be very helpful G Suite Support, [REDACTED]: I  
> just notified the agent so he will contact you if there's something  
> new about it G Suite Support, [REDACTED] can you confirm your phone  
> number Murray McKay: I would really like an update either way - Murray  
> McKay: +[REDACTED] G Suite Support, [REDACTED]: You mean, an update from  
> me? Murray McKay: no from the tier 2 contact G Suite Support, [REDACTED]:  
> Oh, yes I just placed the note to notify the agent and send you an  
> email with the update G Suite Support,  
> [REDACTED] So please keep an eye in your inbox Murray McKay: thank you G  
> Suite Support, [REDACTED]: Sorry for the delays G Suite Support, [REDACTED]:  
> For now is there anything else I can help you with? Murray McKay: no  
> thats it. thanks G Suite Support, [REDACTED]: Thanks for chatting with Google Cloud Support!  
> Keep in mind that you have 30 days to reopen this case if further  
> assistance is needed.  
> -----  
>  
>  
> \*Google Cloud Support\*  
> <https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsupport.google.com%2Fgooglecloud%2Fapps%2F&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&data=7s8nua12xx8fYOxFvKz%2BAGMqwyyh8Oi%2BJs3w3Og%2FEI%3D&reserved=0>  
> <<https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsupport.google.com%2Fgooglecloud%2Fapps%2F&data=02%7C01%7C%7C03b2c42a422e49c5a74208d8455b70c4%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637335606326015314&sdata=0Ha7toKFEvXaSGvfSFeXjNREn%2FtTXtC6CIgKr9pQ5mw%3D&reserved=0>>  
>  
>  
>  
>  
>  
>  
>  
>  
>  
> \*Murray McKay | Director, Digital Literacies\*

>

> T: +61 2 620 \*59756\* | E: murray.mckay@act.gov.au

>

> Digital Strategy, Services & Transformation | Education | ACT

> Government

>

> 51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

>

> <http://www.education.act.gov.au/> | Facebook

> <<https://aus01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.facebook.com%2Fpages%2FACT-Public-Schools%2F94038489456%3Fref%3Dts&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&data=li4NsJ8ZMZxVHN%2BnSz5wCigFCzqKuQJEyxb1QqnbL9Y%3D&reserved=0>>

> | Twitter

> <<https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FACTEducation&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&data=xa7pNyib7TU4lvpYl6l0d2QueenmoV%2FCiVkbCTjv%2BjVA%3D&reserved=0>> | Instagram

> <<https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.instagram.com%2Factpublicschools%2F&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&data=8pAmQ8fYcff1Jcb4Nka%2FHjtXiS0FBdARy2NX4b1%2BzFc%3D&reserved=0>> | LinkedIn

> <<https://aus01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.linkedin.com%2Fcompany%2F706896%3Ftrk%3Dtyah&data=02%7C01%7C%7Cd71922a3895e4740dcaa08d847e54245%7Cb46c190803344236b978585ee88e4199%7C0%7C0%7C637338397271416806&data=LyivNrQ2%2BblzIt4krWtV3lU8ULYrOq4YbS%3Du83tK9I34%3D&reserved=0>>

>

>

>

>

>

>

>

> \*From:\* Bartlett, Kelly <Kelly.Bartlett@act.gov.au>

> \*Sent:\* Friday, 21 August 2020 9:16 AM

> \*To:\* [redacted]@google.com>

> \*Cc:\* [redacted]@google.com>; Bayliss, Michael <Michael.Bayliss@act.gov.au>; McKay, Murray <Murray.McKay@act.gov.au>; Williamson, Bill (ACTEDU) <Bill.Williamson@ed.act.edu.au>

> \*Subject:\* RE: Purge Job

>

>

>

> OFFICIAL

>

>

>

>

> Thank you

>

>

>

>

> Regards,

>

>

>

> \*Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)\*

>

> T: +61 2 620 \*75663\* | M: 0422 233 772 | E: kelly.bartlett@act.gov.au

>  
> Digital Strategy, Services & Transformation | Education | ACT  
> Government  
>  
> 51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
>  
> <http://www.education.act.gov.au/>  
>  
>  
>  
>  
>  
>  
>  
> \*From:\* [REDACTED]@google.com>  
> \*Sent:\* Friday, 21 August 2020 9:14 AM  
> \*To:\* Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
> \*Cc:\* [REDACTED]@google.com>; Bayliss, Michael <  
> Michael.Bayliss@act.gov.au>; McKay, Murray <Murray.McKay@act.gov.au>;  
> Williamson, Bill (ACTEDU) <Bill.Williamson@ed.act.edu.au>  
> \*Subject:\* Re: Purge Job  
>  
>  
>  
> \*CAUTION:\* This email originated from outside of the ACT Government.  
> Do not click links or open attachments unless you recognise the sender  
> and know the content is safe.  
>  
>  
>  
> Hi Kelly,  
>  
>  
>  
> [REDACTED] is looking into the case as we speak... will report back shortly.  
>  
>  
>  
>  
>  
>  
>  
> Best,  
>  
> [REDACTED]  
>  
>  
>  
> On Fri, Aug 21, 2020 at 8:46 AM Bartlett, Kelly  
> <Kelly.Bartlett@act.gov.au>  
> wrote:  
>  
> OFFICIAL  
>  
>  
>  
> Hi Everyone  
>  
>  
>  
> Have we heard anything from the USA team- ideally if we can have an  
> email update this morning and then discuss at 10:30am  
>  
>  
>

> Regards,  
>  
>  
>  
> \*Kelly Bartlett | A/G Executive Branch Manager (Chief Information  
> Officer)\*  
>  
> T: +61 2 620 \*75663\* | M: 0422 233 772 | E: kelly.bartlett@act.gov.au  
>  
> Digital Strategy, Services & Transformation | Education | ACT  
> Government  
>  
> 51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601  
>  
> <http://www.education.act.gov.au/>  
>  
>  
>  
>  
>  
>

> -----  
> - This email, and any attachments, may be confidential and also  
> privileged.  
> If you are not the intended recipient, please notify the sender and  
> delete all copies of this transmission along with any attachments  
> immediately. You should not copy or use it for any purpose, nor  
> disclose its contents to any other person.  
> -----

> -  
>  
>  
>  
>  
>  
> --  
>  
> [Redacted]  
>  
> Google for Education  
>  
> [Redacted]  
>  
>  
>  
>  
>

-----  
This email, and any attachments, may be confidential and also privileged. If you are not the intended recipient, please notify the sender and delete all copies of this transmission along with any attachments immediately. You should not copy or use it for any purpose, nor disclose its contents to any other person.  
-----

ref:\_00D00VNwG.\_5005w1cN6oq:ref

**From:** [Williamson, Bill](#)  
**To:** [Bartlett, Kelly](#); [Bayliss, Michael](#)  
**Cc:** [Ruecroft, Daniel](#); [Valtas, Julian](#); [Sanderson, Mark](#)  
**Subject:** Re: Email activated  
**Date:** Monday, 24 August 2020 11:01:24 PM  
**Attachments:** [image001.png](#)

---

Thanks Michael

Get [Outlook for Android](#)

---

**From:** Bayliss, Michael <Michael.Bayliss@act.gov.au>  
**Sent:** Monday, August 24, 2020 10:03:10 PM  
**To:** Bartlett, Kelly (ACTGOV) <Kelly.Bartlett@act.gov.au>; Williamson, Bill <Bill.Williamson@ed.act.edu.au>  
**Cc:** Ruecroft, Daniel (ACTGOV) <Daniel.Ruecroft@act.gov.au>; Valtas, Julian (ACTGOV) <Julian.Valtas@act.gov.au>; Sanderson, Mark (ACTGOV) <Mark.Sanderson@act.gov.au>  
**Subject:** RE: Email activated

OFFICIAL

Hi Kelly,  
 Dan and I have disabled Gmail for all the OUs except the student OUs where it was previously intended to be on. Staff OUs were also inheriting the 'on' setting, now turned off.  
 Cheers,  
 Michael

---

**From:** Bartlett, Kelly <Kelly.Bartlett@act.gov.au>  
**Sent:** Monday, 24 August 2020 9:03 PM  
**To:** Bayliss, Michael <Michael.Bayliss@act.gov.au>; Williamson, Bill (ACTEDU) <Bill.Williamson@ed.act.edu.au>  
**Cc:** Ruecroft, Daniel <Daniel.Ruecroft@act.gov.au>; Valtas, Julian <Julian.Valtas@act.gov.au>; Sanderson, Mark <Mark.Sanderson@act.gov.au>  
**Subject:** Re: Email activated  
 Hi Michael  
 Yes please. Happy to pick this up in the morning  
 Get [Outlook for iOS](#)

---

**From:** Bayliss, Michael <[Michael.Bayliss@act.gov.au](#)>  
**Sent:** Monday, August 24, 2020 8:39:50 PM  
**To:** Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](#)>; Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](#)>  
**Cc:** Ruecroft, Daniel <[Daniel.Ruecroft@act.gov.au](#)>; Valtas, Julian <[Julian.Valtas@act.gov.au](#)>; Sanderson, Mark <[Mark.Sanderson@act.gov.au](#)>  
**Subject:** RE: Email activated

OFFICIAL

Hi Kelly & Bill  
 I've checked the settings – it looks like Gmail is now on for all students except the individual students which have been moved into NO\_GMAIL OUs – would you like me to turn Gmail off the year levels which previously were set to 'off' before the incident?  
 Cheers,  
 Michael

---



**From:** Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>

**Sent:** Monday, 24 August 2020 8:08 PM

**To:** Ruecroft, Daniel <[Daniel.Ruecroft@act.gov.au](mailto:Daniel.Ruecroft@act.gov.au)>; Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; Valtas, Julian <[Julian.Valtas@act.gov.au](mailto:Julian.Valtas@act.gov.au)>; Sanderson, Mark <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>

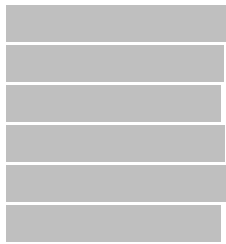
**Cc:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>

**Subject:** Email activated

Hi all,

Gmail has been reactivated on the root OU.

In addition, the following students have had a SUB OU created called "NO\_GMAIL" which has gmail deactivated. We should find a better solution for this, but it had to be done in order to turn it back on.



Things to "unwind" tomorrow

- Delegation settings
- 15 student accounts set up with delegation
- Sub OUs for said 15 accounts manually enabling gmail

**Bill Williamson | Senior Director**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

cid:image002.png@01D4E953.9786AC90

**Education Directorate**

UNCLASSIFIED

<b>To:</b>	Director-General	Tracking No.: EDU 20/1291
<b>Date:</b>	24/08/2020	
<b>CC:</b>	Executive Group Manager, Service Design and Delivery Executive Group Manager, School Improvement	
<b>From:</b>	A/g Executive Branch Manager, Chief Information Officer, Digital Strategy, Services and Transformation	
<b>Subject:</b>	Inappropriate Email Distribution ICT response: Phase Two - approach to restoring Gmail services for all students	
<b>Critical Date:</b>	25/08/2020	
<b>Critical Reason:</b>	To provide confidence to enable the reinstatement of the system	

**Recommendations**

That you:

1. Note the information contained in this brief;

**Noted / ~~Please Discuss~~**

2. Agree to Phase Two - reactivation of accesses to the Gmail services for all students.

**Agreed / ~~Not Agreed / Please Discuss~~**

.....  ..... 24/08/20

**Executive Feedback**

*Approved.*

*I have marked up a couple of changes to the Comms materials on the understanding that the restoration won't be instantaneous.*

*Are you now doing a brief for the Minister to note/endorse my decision? Have you let Bec know? Would you like me to speak to Josh?*

UNCLASSIFIED

UNCLASSIFIED

*Please ask Comms to also do a tweet for me. Same issue with the positioning of 'has been restored/is being restored' in schools.*

## Background

1. On 14 August 2020, an email incident occurred across the ACT public school Google platform resulting in the distribution of group emails (including some containing inappropriate material) to students using their Gmail accounts on the Google Suite for Education (GSFE). The Education limited user access to the GSFE, including Gmail to prevent further escalation of the issue.
2. The Education Directorate investigated the issue determining that the emails were generated by students, starting when a student attempted to share their work with their classmates, accidentally using a Global Distribution list. Other students 'replied all' and a small number of students shared inappropriate content (ref EDU20/1253).
3. The Education Directorate agreed to undertake a two phased approach to re-establish access to the GSFE for all ACT public school students:
  - a. Phase 1 - Reactivation of accesses to the Google Drive and Google Classroom
  - b. Phase 2 - Reactivation of accesses to Gmail
4. Foresight Consulting was engaged to provide an additional layer of risk assurance across both phases.

### Phase One – reactivation of accesses to the Google Drive and Google Classroom

5. Phase 1 – Reactivation of accesses to the Google Drive and Google Classroom, was approved by the DG Monday 17 August 2020 EDU20/1253.
6. The Minister for Education and Early Childhood Development endorsed (MIN20/1289) the restoration of the Google Drive and Google Classroom (Phase one) for all students on Monday 17 August. The Platform (except Gmail) was enabled at 10pm.
7. As part of the decision to restore access to Google Drive and Google Classroom (phase one), it was agreed that DSST would initiate planning for phase two – the reactivation of Gmail. DSST has worked with SSICT, Foresight and Google to ensure that both phases of the GSFE restoration is appropriately addressed from a security perspective and that independent verification has been received around the process.
8. Phase one required that the collaboration settings in Google were reviewed and improved, and that appropriate controls were put in place to ensure the removal of student access to global distribution lists. This enabled the safe reinstatement of Google Drive and Google Classroom access.
9. Following the decision to restore access, real time monitoring by DSST staff has occurred for a period of three days, with a possibility of extension. This has further ensured the adequacy of the security controls implemented for Google Drive and

UNCLASSIFIED

UNCLASSIFIED

Google Classroom.

Phase Two – reactivation of accesses to Gmail

10. The reactivation of accesses to Gmail requires a specific plan for data preservation, restoration and analytical setup. It was designed to ensure that all 16.5M emails that were sent over the 14 August 2020 were extracted from students' Gmail accounts and that additional security measures were put in place including alerts and monitoring of mass emailing, restrictions around the number of recipients and an internal email filter system.
11. The Directorate has continued to work closely with Google and Foresight, in order to support the reinstatement of Gmail.
12. Each step, including the restoration of Google Drive and Google Classroom, has been monitored and has been tested to ensure it is robust and verified by an independent consultant. The activities and dates are outline in Attachment A – Gmail Reactivation Detailed Activity List
13. The Directorate has confirmed that the following actions have occurred in order to enable the restoration of Gmail. All cross checking has been completed across several year levels and includes primary/secondary/college students, and at least two schools per stage.

***Tier 1 (Mandatory)***

- a) No emails from 10.00hrs Friday 14 August 2020 are available to students  
**(COMPLETED)**
- b) Alerting and Controls **(COMPLETED)**:
  - a. Ensuring that Global Groups is turned off
  - b. Ensuring that the Global Distribution list is blocked
  - c. Ensuring that Auto Complete (for email addresses) is turned off
  - d. Internal email filter updated
  - e. Alerts and monitoring for mass email events including new email parameters (limiting the number of recipients)
- c) Foresight consulting assurance for phase two reactivation of Gmail readiness.  
**(COMPLETED)**

***Tier 2 (Desirable)***

- a) Data transfer for audit purposes and containing this information in a 'read only' Google Vault. **(sample size of 50,000 COMPLETED)**

UNCLASSIFIED

## UNCLASSIFIED

- b) Confirm that a process to retrieve any 'lost' email is in place and has been tested. **(COMPELTED)**
14. The directorate will retrieve any emails that have been deleted, through the ITO's placing a request to DSST. DSST will utilise Google services to restore the email. This process will be communicated to Principals, IT Officers and IT Coordinators Monday 24 August 2020.
15. The Directorate has had multiple experts involved in this process including:
- a) Education Directorate Staff
  - b) Shared Services ICT embedded team and security team
  - c) Googles preferred technical partner: Geeks on Tap
  - d) Foresight Consulting assurance
  - e) Google for Education support team
16. To support the controls put in place, the Directorate has met with Foresight Consulting completing screen shares and provided testing logs and scripts to a satisfy an independent third-party assurance verification.
17. Foresight Consulting has reviewed this process and has provided assurance that the testing is robust, and that the approach is sufficient to eliminate the risk of a similar incident taking place (Attachment B). An excerpt of Foresight Consulting readiness for reactivation of Phase 2 - Gmail services is below:
- "Foresight assess that ACT Education have undertaken appropriate measures to mitigate exposure of inappropriate content to students and that the risk of a mass email incident reoccurring has been minimised. ACT Education would be in a position based on its actions taken to date, to re-enable Gmail services."*
18. DSST is confident that the issue has been appropriately addressed from a security perspective and this has been independently verified by Foresight Consulting. It is therefore recommended that the Director-General approve the restoration of Gmail services and access to all students. It is proposed that the Gmail services be restored on Monday evening 24 August 2020. Google may require 24 hours to fully process the action.
19. DSST will activate Gmail school by school, commencing with Colleges, High schools finishing with Primary schools.
20. Following the decision to restore access to Gmail, DSST will continue the real-time monitoring of the new security enhancements to ensure that they are robust and sound.

UNCLASSIFIED

## UNCLASSIFIED

**Issues**

21. Google services encountered a service degradation issue on Thursday 20 August 2020 that impacted ACT Educations ability to continue purge job.
22. The purging of emails involved in this incident was initially anticipated to take approximately two hours. The purging activity has taken more than four full days.
23. Google services can take between 30 minutes to 24 hours to fully activate.

**Financial Implications**

24. The Education Directorate has engaged Foresight Consulting to assist at an hourly rate of [REDACTED] (inclusive of GST).

**Consultation**Internal

25. Service Design and Delivery Group has worked closely with School Improvement Group to manage this incident and communications with schools and families.
26. The Media and Communications and Complaints Handling teams have been informed with respect to the email incident and are providing support with communications to schools, students and their families.

Cross Directorate

27. The Education Directorate has worked closely operationally with Shared Services ICT, to ensure that the ICT security measures being taken aligned with WhoG approaches.
28. The Education Directorate notified the ACT Government Chief Digital Officer.

External

29. The Education Directorate notified the Australian Federal Police and Office of the eSafety Commissioner.
30. The Education Directorate engaged Foresight Consulting to assist with risk and assurance activities.
31. The Education Directorate engaged Google for Education support team services.
32. The Education Directorate engaged Geeks on Tap for additional Google advice and support services.

**Work Health and Safety**

33. Nil.

**Benefits/Sensitivities**

34. Concerns have been raised about the impact on assessment for Year 11 and 12 students due to their GSFE access being removed. Preliminary investigations indicate

UNCLASSIFIED

## UNCLASSIFIED

that the students who disseminated inappropriate material were from this cohort of students.

### Communications, media and engagement implications

35. The Education Directorate has been working closely with the Minister's Office, media outlets, managing social media and managing communications to the public.
36. The Education Directorate issued letters to parents on Friday 14 August 2020 and 17 August 2020 providing details of the event, the temporary unavailability of the GSFE and the measures being undertaken to provide security assurance.
37. There have been several social media posts targeting college students and their families.
38. The Education Directorate issued letters and provided other communication (including teleconferences) to school leaders and business managers on Friday 14 August 2020, Sunday 16 August 2020 and Monday 17 August 2020. With an update communications pack scheduled for Monday 24 August 2020, once reactivation has been approved.

Signatory Name: Ross Hawkins

Phone:

Action Officer: Kelly Bartlett

Phone:

### Attachments

Attachment	Title
Attachment A	Gmail Reactivation Detailed Activity List
Attachment B	Foresight Consulting assurance email for Phase two

UNCLASSIFIED

## Attachment A – Detailed Activity List

### Acceptance criteria

#### Confirmation Protocol:

- All cross checking has been complete across a number of year levels and includes Primary / Secondary / College and at least 2 schools per stage.

#### Tier 1 (Mandatory):

Description	Status
- Confirm that no emails from 10AM 14 August are available to students (15 student cross check complete)	Confirmed. Checked with 23 student accounts
- Confirm that EDU can verify that new security settings are in place and verified. <ul style="list-style-type: none"> <li>o Global list blocking</li> <li>o Auto complete</li> <li>o Alerts and monitoring are installed</li> <li>o Internal email filter has been updated</li> </ul>	Confirmed and tested
- That Foresight has provided assurance that the testing is robust and that this approach is sufficient to eliminate the risk of a similar incident taking place.	Refer email

#### Tier 2 (Desirable)

Description	Status
- Confirm that a version of the data is securely stored and available for Audit purposes. (15 student cross check complete)	Tested with 50,000 messages (includes all sent)
- Confirm that a process to retrieve any 'lost' email is in place and has been tested.	Process confirmed, part of comms pack and has been tested



## Daily Activity Run Sheet Update

## Tuesday (Data transfer for Audit purposes)

Description	Status
- Confirmed approx. 16.5M emails generated over 14 <sup>th</sup> Aug period.	Confirmed 16.5mil emails received by students 18/8
- Noting former extraction method failed, reinstate new retrieval process for all email (14 <sup>th</sup> August)	Confirmed 18/8
- Agree new extraction methodology with Google.	Agreed 18/8
- Initiate process to store emails in 'Google Vault' - (three step process). Will need assurance that all emails are in the vault before deletion (ensuring security parameters with Google). <b>Also ensure this data is Read Only.</b>	Initiated 18/8
- Sample run at least 30 (to verify and check)	Verified 18/8

## Wednesday (cleansed data and creating scripts / setting for new approach)

Description	Status
- Further consultation (and finalisation) with Google on further email control parameters.	Completed x2 19/8
- Develop alerts and monitoring approach and internal email filter	Approach agreed. Draft scripts Ready to be deployed. Will be deployed and tested tomorrow morning. 19/8
- Initiate data cleansing (will require hours).	Commenced 19/8
- Verification that data cleansing was successful.	Purge jobs ran until Sunday 23 August 2020. Validated that All Email Messages have been purged
- Run the 'blocking' scripts (developed over the weekend) for Drive and Classroom.	Completed and tested 19/8
- <b>Send first set of assurance and Script information to Foresight.</b>	Several meetings (daily) 24/8
- Develop Comms (focused on Gmail back up and security enhancements in place): <ul style="list-style-type: none"> <li>o For Principals and ITOs</li> <li>o For Community</li> <li>o Socials</li> </ul>	Developed and EGM SDD for approved 24/8
- Provide guide for students and families on sync of devices and checking for corruption	Developed. Validated with selected pilot student group 24/8
- Stakeholder discussions	EGM SDD stakeholder engagement P&C 19/8
- Wednesday evening – check in with Ministers office	EGM SDD check in MO 17:30.

**Thursday (Testing and verification with assurance partner)**

Description	Status
- Test and verify the outcomes (that global groups are blocked).	Tested - Successful
- Test auto complete process is blocked.	Tested - Successful
- Test new alert and monitoring processes and internal email filter.	Tested - Successful
- <b>Run through scripting and testing outcomes with Foresight for assurance.</b>	Several Meetings, and evidence provided
- DG Brief and Ministerial Brief – Seeking approval to bring Gmail back online.	EDU20/1291 and MIN20/1304

**Friday**

Description	Status
- Approval of Minister Brief and green light Gmail.	Rescheduled to Monday 24 August
- Turn on Gmail. Google may require 24 hours to fully process.	Rescheduled to Monday night 24 August 2020

**From:** [REDACTED]  
**To:** [Bartlett, Kelly](#)  
**Cc:** [REDACTED]  
**Subject:** Ongoing analysis of incident approach and Phase Two enabling of services [OFFICIAL]  
**Date:** Monday, 24 August 2020 12:27:28 PM  
**Attachments:** [image001.png](#)

---

**CAUTION:** This email originated from outside of the ACT Government. Do not click links or open attachments unless you recognise the sender and know the content is safe.

## OFFICIAL

Hi Kelly,

Foresight have continued to review and assess ACT Education's incident management approach in response to the email incident. The mitigating controls and recovery of services approach and testing undertaken are considered appropriate for ACT Education's Phase two plan to re-enable Gmail services. This conclusion is based on assessment and evidence observed between Friday 14 August 2020 through to Monday 24 August 2020.

Based on Foresight's assessment, several areas have been considered and addressed by ACT Education which Foresight have deemed to be appropriate to mitigate the risk of the incident reoccurring:

- Distribution lists created by an auto copy process from Active Directory, discovered by ACT Education to have made up the root cause of the incident, have been deleted.
- ACT Education have removed students from all distribution lists in the environment.
- Testing has been undertaken using student profiles to ensure that appropriate security controls are in place to prevent mass email situations.
- ACT Education are working with Google directly to ensure that investigation evidence is maintained.
- ACT Education have setup an appropriate evidence storage environment that will be used for future investigations and long term archiving of evidence data.
- Removal of emails sent from 10am onwards on the day of the incident has been undertaken to purge all instances of inappropriate content. Legitimate emails from the day can be recovered upon request. ACT Education have undertaken testing to validate this approach.
- ACT Education have undertaken manual verification of any remaining emails from the day of the incident in student inboxes. This further minimises the risk of residual inappropriate content that may have been missed from the global purge job.
- Google Drive collaboration settings have been updated so that all student accounts are disabled from sharing content, whilst teachers are exempted.
- ACT Education are documenting the steps undertaken during the incident and to assist in preserving the integrity of incident evidence captured.
- Manual monitoring is being put in place by ACT Education staff to observe and minimise the risk of incident reoccurrence. ACT Education are considering a long term monitoring solution for the environment.

Whilst Foresight recommend ACT Education have a completed and verified export of all emails from the day of the incident, it is understood that Google have provided formal assurance in writing that email evidence is being held indefinitely and can be exported for investigation.

Foresight assess that ACT Education have undertaken appropriate measures to mitigate exposure of inappropriate content to students and that the risk of a mass email incident reoccurring has been minimised. ACT Education would be in a position based on its actions taken to date, to re-enable Gmail services.

Regards,

[Redacted signature block]

[Redacted signature block] [@foresightconsulting.com.au](mailto:[Redacted]@foresightconsulting.com.au)



This message is intended for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. Any unauthorized use, distribution, or disclosure is strictly prohibited. If you have received this message in error, please notify sender immediately and destroy/delete the original transmission

OFFICIAL

Classified by [Redacted] @foresightconsulting.com.au on 24/08/2020 12:26:42 PM

**From:** [Kaur, Puneet](#)  
**To:** [Bartlett, Kelly](#); [Williamson, Bill \(ACTEDU\)](#); [McKay, Murray](#)  
**Cc:** [Bayliss, Michael](#); [Ruecroft, Daniel](#); [Sanderson, Mark](#); [Valtas, Julian](#); [Southwell, Mark](#); [Gerbich, Leon](#)  
**Subject:** RE: Google - Activation of Gmail services  
**Date:** Wednesday, 26 August 2020 9:23:38 AM  
**Attachments:** [image002.png](#)  
[image003.png](#)

**OFFICIAL: Sensitive**

Thank you for the update [@Bartlett, Kelly](#)

Is there any update on turning ON the google sync from AD. At this stage we are manually editing student and staff's google account based on the requests however we still receiving cases of new enrolments requiring google account.

Kind Regards.

Puneet Kaur | Senior Business System Support Officer | Education ICT

**Phone:** +61 2 620 75774 | **Email:** [Puneet.Kaur@act.gov.au](mailto:Puneet.Kaur@act.gov.au)

**Customer Engagement Services Branch | Shared Services ICT | Chief Minister, Treasury and Economic Development Directorate | ACT Government**

51 Fremantle Drive, Stirling, ACT 2611 | GPO Box 158 Canberra ACT 2601 | [www.act.gov.au](http://www.act.gov.au)

*Please consider the environment before printing this email. If printing is necessary, print double-sided and black and white.*



**From:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>

**Sent:** Monday, 24 August 2020 8:15 PM

**To:** Bayliss, Michael <[Michael.Bayliss@act.gov.au](mailto:Michael.Bayliss@act.gov.au)>; Ruecroft, Daniel <[Daniel.Ruecroft@act.gov.au](mailto:Daniel.Ruecroft@act.gov.au)>; Sanderson, Mark <[Mark.Sanderson@act.gov.au](mailto:Mark.Sanderson@act.gov.au)>; Valtas, Julian <[Julian.Valtas@act.gov.au](mailto:Julian.Valtas@act.gov.au)>; Southwell, Mark <[Mark.Southwell@act.gov.au](mailto:Mark.Southwell@act.gov.au)>; Kaur, Puneet <[Puneet.Kaur@act.gov.au](mailto:Puneet.Kaur@act.gov.au)>; Gerbich, Leon <[Leon.Gerbich@act.gov.au](mailto:Leon.Gerbich@act.gov.au)>

**Cc:** Williamson, Bill (ACTEDU) <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>

**Subject:** FW: Google - Activation of Gmail services

**OFFICIAL: Sensitive**

FYI – the Gmail services has been reactivated tonight

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 75663 | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)

**From:** Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>

**Sent:** Monday, 24 August 2020 8:09 PM

**To:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>; McKay, Murray <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Bellchambers, Jay (ACTEDU) <[Jay.Bellchambers@ed.act.edu.au](mailto:Jay.Bellchambers@ed.act.edu.au)>; Crawford, Jodie <[Jodie.Crawford@act.gov.au](mailto:Jodie.Crawford@act.gov.au)>; Tiruchi, Shakir <[Shakir.Tiruchi@act.gov.au](mailto:Shakir.Tiruchi@act.gov.au)>; McMahon, Zoe <[Zoe.McMahon@act.gov.au](mailto:Zoe.McMahon@act.gov.au)>; Smith, Tracey Lee <[TraceyLee.Smith@act.gov.au](mailto:TraceyLee.Smith@act.gov.au)>; Armstead, Paul <[Paul.Armstead@act.gov.au](mailto:Paul.Armstead@act.gov.au)>; Spencer, David (ACTEDU) <[David.Spencer@ed.act.edu.au](mailto:David.Spencer@ed.act.edu.au)>; Pearson, Andrew (ACTEDU) <[Andrew.Pearson@ed.act.edu.au](mailto:Andrew.Pearson@ed.act.edu.au)>

**Cc:** Dissanayake, Avon <[Avon.Dissanayake@act.gov.au](mailto:Avon.Dissanayake@act.gov.au)>; Crossley, Nick

<[Nick.Crossley@act.gov.au](mailto:Nick.Crossley@act.gov.au)>; Bessey, Rochelle <[Rochelle.Bessey@act.gov.au](mailto:Rochelle.Bessey@act.gov.au)>; van der Walt, Robeya <[Robeya.vanderWalt@act.gov.au](mailto:Robeya.vanderWalt@act.gov.au)>

**Subject:** RE: Google - Activation of Gmail services

Hi all,

Worth noting is it MAY take up to 24 hours for all accounts to be reactivated. Keep this in mind with the support calls etc.

**Bill Williamson | Senior Director**

T: 0430 333 647 | E: [bill.williamson@ed.act.edu.au](mailto:bill.williamson@ed.act.edu.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au) | [Facebook](#) | [Twitter](#) | [Instagram](#) | [LinkedIn](#) | [Google+](#)

---

**From:** Bartlett, Kelly <[Kelly.Bartlett@act.gov.au](mailto:Kelly.Bartlett@act.gov.au)>

**Sent:** Monday, 24 August 2020 8:07 PM

**To:** McKay, Murray (ACTGOV) <[Murray.McKay@act.gov.au](mailto:Murray.McKay@act.gov.au)>; Williamson, Bill <[Bill.Williamson@ed.act.edu.au](mailto:Bill.Williamson@ed.act.edu.au)>; Bellchambers, Jay <[Jay.Bellchambers@ed.act.edu.au](mailto:Jay.Bellchambers@ed.act.edu.au)>; Crawford, Jodie (ACTGOV) <[Jodie.Crawford@act.gov.au](mailto:Jodie.Crawford@act.gov.au)>; Tiruchi, Shakir (ACTGOV) <[Shakir.Tiruchi@act.gov.au](mailto:Shakir.Tiruchi@act.gov.au)>; McMahon, Zoe (ACTGOV) <[Zoe.McMahon@act.gov.au](mailto:Zoe.McMahon@act.gov.au)>; Smith, Tracey Lee (ACTGOV) <[TraceyLee.Smith@act.gov.au](mailto:TraceyLee.Smith@act.gov.au)>; Armstead, Paul (ACTGOV) <[Paul.Armstead@act.gov.au](mailto:Paul.Armstead@act.gov.au)>; Spencer, David <[David.Spencer@ed.act.edu.au](mailto:David.Spencer@ed.act.edu.au)>; Pearson, Andrew <[Andrew.Pearson@ed.act.edu.au](mailto:Andrew.Pearson@ed.act.edu.au)>

**Cc:** Dissanayake, Avon (ACTGOV) <[Avon.Dissanayake@act.gov.au](mailto:Avon.Dissanayake@act.gov.au)>; Crossley, Nick (ACTGOV) <[Nick.Crossley@act.gov.au](mailto:Nick.Crossley@act.gov.au)>; Bessey, Rochelle (ACTGOV) <[Rochelle.Bessey@act.gov.au](mailto:Rochelle.Bessey@act.gov.au)>; van der Walt, Robeya (ACTGOV) <[Robeya.vanderWalt@act.gov.au](mailto:Robeya.vanderWalt@act.gov.au)>

**Subject:** Google - Activation of Gmail services

OFFICIAL: Sensitive

Hi Everyone

Just a quick note to let you know that we are activating Gmail services tonight. In the morning we will touch base on:

- Comms to ITO and ITC's
- Expected behaviour of personal devices
- Email retrieval process
- Alerting and Monitoring

Key items to note

- we have deleted all emails post 10am Friday 14 August.
- We have removed all students out of Groups
- We have disabled the address book auto population
- We have limited the students ability to email more than 30 address per message
- Updated the rude work list and alerts for attachments

Any questions, please let me know.

Regards,

**Kelly Bartlett | A/G Executive Branch Manager (Chief Information Officer)**

T: +61 2 620 **75663** | M: 0422 233 772 | E: [kelly.bartlett@act.gov.au](mailto:kelly.bartlett@act.gov.au)

Digital Strategy, Services & Transformation | Education | ACT Government

51 Fremantle Drive, Stirling ACT 2611 | GPO Box 158, Canberra ACT 2601

[www.education.act.gov.au](http://www.education.act.gov.au)





## Caveat Brief

**To:** Minister for Education and Early Childhood Development  
**From:** Ross Hawkins – Executive Group Manager – Service Design and Delivery  
**Subject:** Student email incident – communications activities  
**Date:** 22 August 2020

That you note the activities to date.



Noted / Please discuss

Yvette Berry MLA 26/8/20

### Overview

- In responding to the email incident of 14 August 2020, the Education Directorate has been providing supports to schools, students and their families (reference MIN20/1275).
- Caveat brief (MIN20/1289) set out a 2 phased approach:
  - Phase one - Reactivation of accesses to the Google Drive and Classroom
  - Phase two - Reactivation of accesses to Gmail
- Foresight Consulting was engaged by the Education Directorate to provide an additional layer of risk assurance across both phases.
- Phase 1 - Google Drive and Classroom were successfully enabled 22.00hrs 17 August 2020. Schools have been utilizing the Google services since Tuesday. Directorate staff have been undertaking real-time monitoring during this period to ensure that the processes undertaken are robust and sound.

### Technical solution to Phase 2.

- With advice from our technical partners we anticipated that the Gmail purge process of the 16.5 million messages generated between 10am and 1pm on the 14<sup>th</sup> August would take a few hours to complete. The purge job commenced Wednesday 19<sup>th</sup> August at 5pm. After the first 12 hours (overnight) only 4% of messages had been purged. The Directorate escalated and worked closely with Google who has been assisting with expediting the job.
- As at 10 am on Saturday 22 August, with Google's assistance the purging rate has increased significantly however approximately 13% of emails remain.
- It is expected that the remaining emails will be purged by 5 pm on Saturday, and that the Directorate team will then resume work tomorrow to confirm that the deletion has occurred with random testing and assurance. We will then seek external assurance from Foresight on Monday, as we did for the previous elements of the restitution project.
- You will then be briefed with the outcome of the process and external assurance to reconnect email and have available from Tuesday.

- Note that this proposed timing – notwithstanding Google’s assistance – means that the most likely timing for reconnection of Gmail is Tuesday (not Monday). This is in order to
  - (A) build in additional time for checking and assurances; and
  - (B) take into account the fatigue of the EDU workers who have been working on this without a break since last Friday.
- We consider that this timeframe is manageable as schools and the community have not been applying pressure to reinstate Gmail, as they did for the Google Drive and Google Classroom services.

#### Communication with Impacted Students and Families

- The Directorate has spoken with the family identified in the Canberra Times article, regarding [REDACTED] and offered support.

- Schools have been in contact with the suspended students [REDACTED] in total) this week and provided school-based work. The students and families have been provided with the Telehealth number and asked to get in contact if they require any further support.
- For one of the students (at [REDACTED]), upon request, the school arranged for the school psychologist to make contact with the family.
- Principals have been in touch with the families (Friday 21 August), about the students coming back to school on Monday 24<sup>th</sup> August. Discussions will take place with students and parents relating to the reasons they were suspended, outlining their breach of the ICT agreement.
- Students will be provided access to Google Drive and Classroom (but not Gmail when services resume) and advised that their accounts will be monitored.
- Students will be requested not to use their personal devices at school.
- The school will highlight that there will be a further discussion once the police investigation is finalised.

#### Communication with AFP, eSafety Commissioner and Parents and Cares Association

- Discussions with the P&C have highlighted their enthusiasm to work with the Directorate, eSafety Commissioner and AFP on conducting community sessions. It is likely we can run a collaborative session after child protection week.
- The AFP are continuing to work through the evidence packs provided on the [REDACTED] suspended students activities. They have confirmed that they will interview students and have agreed with the Directorates approach to students outlined above.

#### Communication with Community

- The Directorate published an update to the community through a web story and socials on Friday evening. The message highlighted to the community that we are still working on this issue and will bring Gmail back when we are confident that all emails are deleted and that safety controls are in place.
- A communication pack is ready for when the system can be brought up and these could be activated over the weekend if we need to.
- The Directorate has not received many complaints from the community or reports in from schools over the last 2 days. In total we have had about]



- 20 calls, the majority of these calls were college parents concerned about access to Google Drive and Classroom, impact the students to prepare assignments and complete work.

Signatory Name: Ross Hawkins  
Title Executive Group Manager, Service  
Design and Delivery  
Date 22 August 2020

UNCLASSIFIED



# Major Incident Report

## Inappropriate Emails Circulated through Student Distribution Groups

### Business Systems Impacted

Date Incident Recorded:	14 August 2020, 10:59am
Case Number	Google case number - 24674292
Prepared by:	Kelly Bartlett
Business System	Google Suite - GMail
Criticality	High
Outage	Friday 14 August 2020 – 13:15pm – ongoing
Incident Duration	Friday 14 August 2020 – 10:59am – ongoing

### Incident

#### Business Impact

Students commenced reporting to teachers that they were receiving numerous emails, including inappropriate emails.

#### Issue

The circumstances surrounding the emails include:

- Year 6 student who shared a Google Presentation to an Internet group with all Year 8's across the ACT public school system. This share first occurred to a Distribution List occurred 10:02am Friday 14 August 2020.
- The presentation has been reviewed and is an assignment relating to monkeys. As all shares automatically generate an email, a year 8 student, using Gmail replied all with a comment.
- Appears to have set off a chain of behaviour of other students joining in, which escalated to inappropriate information being shared.
- Students that initiated emails to DL across year groups have been identified
- Students that initiated email with inappropriate emails have been identified and an ongoing review continues.

#### Technical Investigation

- Google default settings allows all to send to all Distribution Groups.
- The distribution groups that have been used were system generated due to:
  - the new Content Keeper web filtering changes were introduced in late April, year Groups are created in Active Directory to ensure the correct web filtering rules are applied to the correct students across the system
  - There is an automatics IDAM Active Directory synchronisation job that copied these groups into Google
  - the system generated a Distribution Group applying the Google default settings, making the groups accessible to all.
  - There is no requirement for these groups to be available in Google

### Summary of Resolution

The Education Directorate undertake a two phased approach to re-establishing access to the GSFE for all ACT public school students. The phases are:

UNCLASSIFIED

UNCLASSIFIED



- Phase 1 - Reactivation of accesses to the Google Drive and Google Classroom
- Phase 2 - Reactivation of accesses to Gmail

Foresight Consulting has been engaged to provide an additional layer of risk assurance across both phases. Engaging an external service provider will ensure that adequate security measures are in place to prevent any likelihood of an incident of this nature occurring in future.

The below chart using a RACI model outlines involvement in each key activity.

- R = Responsible for action
- A = Accountable for action
- C = Consulted
- I = Informed

Phase 1 Details	EDU	SSICT	Google	GoT	Foresight
Systems isolated for Event Review	RA	R	C	C	I
First Event of Email to Distribution List (DL) Identified	RA	R	-	-	I
Cause of Capability Identified	RA	R	-	-	I
Remediation Actions Completed					
Distribution Lists settings change – students cannot send	RA	R	C	C	I
Review of Pre-mutation of Similar Event Completed					
Auto Address Turned Off	RA	I	-	I	I
Students Cannot create Groups	RA	C	-	C	I
Students cannot create Shared Drives	A	R	-	C	I
Update AD Sync to Google	A	R	-	-	I
Rigorous Testing					
Gmail still turned off	RA	-	-	C	I
Google Drive Testing	RA	-	-	C	I
Google Classroom testing	RA	-	-	C	I
Google Meet Testing	RA	-	-	C	I
Google Doc Testing	RA	-	-	C	I
Assurance Report and Review	I	I	I	C	RA

## Recommendations:

The below table outlines actions to be taken to minimise this type of major incident from reoccurring.

#	Recommendation	Date
1	Phased approach to turn on the Google for Education suite: <ul style="list-style-type: none"> <li>• Phase 1 – All services except Gmail – 17 August</li> <li>• Phase 2 – Gmail 22 August</li> </ul>	17 August 22 August
2	Remove all emails shared via DL lists from Student accounts	21 August
3	Additional review step to be introduced for any system changes	17 August
4	Scripts to suspend accounts to be stored in source code and shared with SSICT	Complete
5	Ongoing Monitoring and Alerts to be included	Ongoing

UNCLASSIFIED



Trim No. MIN20/1372

## Caveat Brief

**To:** Minister for Education and Early Childhood Development  
**From:** Katy Haire, Director-General Education Directorate  
**Subject:** Gmail Post Incident Review - Independent Audit

That you endorse the attached Terms of Reference (ToR) for an independent audit to be undertaken following the email incident which occurred on 14 August 2020.

Endorse / Please discuss

Kyelle Berry MLA 10/09/20

- On 14 August 2020, an email incident occurred across the ACT public school Google platform resulting in the distribution of group emails (including some containing inappropriate material) to students using their Gmail accounts on the Google Suite for Education (GSFE).
- On 14 August 2020 you directed the Directorate undertake an independent audit of the incident to ascertain its root cause, and to provide assurance that a similar incident could not happen again. It is proposed an independent audit be undertaken as a priority, commencing in early September 2020.
- The Directorate will use its audit partner PwC to perform this function. PwC has both expertise in audit and assurance, but also cyber security expertise to support this work.
- The audit will undertake a root cause analysis of the incident and identify the impacting factors and make recommendations to ensure that a similar incident cannot recur. It will also evaluate the incident response and implement learnings for future incidents, both from a technical, operational and governance perspective.
- As part of the audit, there will need to be a clear understanding of the management and control of the Google system, including the role of Shared Services ICT.
- The audit objectives, scope, criteria and timeframes are included in the terms of reference at Attachment A.
- The audit terms of reference have been discussed with the Chair of the Audit Committee and the final report will be subject to the Audit Committee's endorsement.

Signatory Name: Katy Haire

Date: 4 September 2020

# Terms of Reference

## *Gmail Post Incident Review*

**DRAFT**

September 2020

DRAFT

# Contents

1	Executive Summary	3
2	Objective and scope	3
3	Approach	4
4	Approval	7

## Disclaimer

This Terms of Reference has been prepared by PricewaterhouseCoopers (PwC) in accordance with the terms of Work Order Number EDU20/505 dated 7 July 2020. This Terms of Reference is solely for the information of the ACT Education Directorate. Its existence may not be disclosed nor its contents published in any way without the prior written approval of PwC. PwC does not accept any responsibility to any other party to whom this Terms of Reference may be shown or into whose hands it may come.

Whilst the work performed may involve the analysis of financial information and accounting records, it does not constitute an audit or review in accordance with Australian Auditing Standards, Standards on Review Engagements or Standards on Assurance Engagements as issued by the Auditing and Assurance Standards Board and accordingly no such assurance will be provided in any of our deliverables.

Liability limited by a scheme approved under Professional Standards Legislation.

# 1 Executive Summary

## Background

This independent audit is to address circumstances that resulted in inappropriate content being distributed by students via group mail distribution lists which became available on Gmail. Technical amendments on network controls resulted in the creation of year group distribution lists, which a student accidentally discovered. With this unintended capability having been exposed, there was a cascading series of emails sent by other students across a variety of group email lists that covered entire year groups across the ACT education system. This has occurred through the Education Directorate's deployment of Gmail for student email.

There is a need for the Directorate to understand what caused the failure in network controls, evaluate the incident response and implement learnings for future incidents, both from a technical and operational and governance perspective. There is also a need for the Directorate to clarify the nature of relationship with Shared Services by way of service level agreements in place to support security controls.

## Strategic Risk Reference

This review is related to the following risks, as detailed within ACT Education's Strategic Risk Register:

- #10 – The Directorate is unable to prevent or actively respond to the management of operational issues at school and system levels

# 2 Objective and scope

The objectives of this independent audit are to:

- a) provide a root cause analysis of the incident, defining what took place, the impacting factors and to provide recommendations to ensure a similar incident cannot take place again
- b) assess the adequacy of governance arrangements in place between ACT Education and Shared Services with respect to ICT administration and response to critical events. This will include a particular focus on clarity of roles, responsibilities and escalation channels; and
- c) evaluate the incident response in terms of appropriateness and timeliness of actions by both the Directorate and Shared Services.

To achieve the objectives, the review will:

- map out the incident in terms of key cascading events and actions taken by ACT Education and Shared Services;
- understand relevant network controls and any points of vulnerability within the Google system, relating to security features;
- review governance arrangements in place between ACT Education and Shared Services, with a focus on roles and responsibilities; and
- identify learnings for future handling of incidents and provide recommendations to strengthen governance and control frameworks (as applicable).

## Scope exclusions

- The review is focussed on the management of risks associated with distribution lists in Gmail for students. The review does not include consideration of broader system or deployment processes.



- The Directorate will share findings from the security review being undertaken by a separate external provider with PwC (as appropriate). PwC will not duplicate work undertaken by this external provider unless instructed to by the Directorate.

## 3 Approach

The review team will undertake the following approach to address the objectives and scope of this review.

### Planning

- Engage with the Review Sponsor to obtain a high-level understanding of the circumstances that resulted in explicit content being distributed by a student via distribution lists which became available on Gmail.
- Develop and agree the review scope with the Review Sponsor.

### Fieldwork

- Meet with relevant management from ACT Education and Shared Services<sup>1</sup> to obtain a detailed understanding of:
  - the incident and actions taken in response by the Directorate and Shared Services; and
  - governance arrangements between ACT Education and Shared Services, including roles, responsibilities and escalation processes.
- Review findings from the separate external security review.
- Review relevant system risk registers to help inform the risk and control environment.
- Review documentation and reporting related to governance arrangements between ACT Education and Shared Services
- Confirm any observations, findings and opportunities for improvement real-time.

### Reporting & Quality

- Confirm the factual basis of review observations with management during the exit meeting.
- Prepare the draft report for management comment.
- Obtain management comments from the Review Sponsor and incorporate into the final report
- Maintain quality assurance processes throughout the review.
- Seek feedback and continually improve on lessons learnt from the review.

### Key Stakeholder Consultation

Key stakeholders are identified in the table below. Additional stakeholders to be consulted with during the review will be identified during planning.

Stakeholder	Role	Scoping	Fieldwork	Exit Meeting
David Matthews	Deputy Director-General, Education Services (and Review Sponsor)	✓		✓

<sup>1</sup> Subject to availability of Shared Services personnel within the review timeframes.



Ross Hawkins	Executive Group Manager, Service Design and Delivery	✓	✓	✓
Kelly Bartlett	A/g Executive Branch Manager, Digital Strategy, Services and Transformation		✓	

## Timetable

This review is expected to require 25 days of effort. No travel is required for this review as all fieldwork will be conducted by Canberra based PwC personnel.

The timing of the review is as follows:

Milestone	Date	Accountability
Scoping Meeting	31 August 2020	PwC / ACT Education
Draft Terms of Reference	3 September 2020	PwC
Agreed Signed Terms of Reference	10 September 2020	PwC / ACT Education
Commence Fieldwork	14 September 2020	PwC
Mid-Point Meeting with Review Sponsor	2 October 2020	PwC
Circulate Discussion Paper	16 October 2020	PwC
Discussion Paper Meeting with Review Sponsor	w/c 19 October 2020	PwC
Issuance of formal Draft Report	30 October 2020	PwC
Management Comments Received from Review Sponsor	10 November 2020	ACT Education
Final Report	13 November 2020	PwC
Endorsement of Final Report	10 December 2020	Audit Committee

This timetable and total review days is based on our understanding of the scope of this review and the availability of relevant ACT Education staff. Should delays occur in the completion of key milestones we will raise them with the Review Sponsor and Chief Internal Auditor to discuss and agree a revised timeline.

## Specified Personnel

The specified personnel from PwC are:

Name	Position

[Redacted]

[Redacted]

[Redacted]

[Redacted]

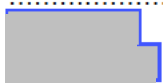
DRAFT

# 4 Approval

The Terms of Reference have been reviewed and approved by:

.....  
David Matthews  
ACT Education  
Deputy Director-General, Education Services

.....  
Date

.....  


.....  
Date

DRAFT

DRAFT

[www.pwc.com.au](http://www.pwc.com.au)

© 2020 PricewaterhouseCoopers. All rights reserved.

PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Liability limited by a scheme approved under Professional Standards Legislation.

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.com.au](http://www.pwc.com.au).

WL 127070755



**FORESIGHT**

CYBER SECURITY • COMPLIANCE & ASSURANCE

# ACT Education – Email Incident

## Post Incident Analysis Report

September 2020

*DOCUMENT CONTROL*

Document title	Email Incident - Post Incident Analysis Report
Prepared for:	ACT Education
Document type:	Post Incident Analysis Report
Version:	1.6
Status:	Final for release to client.
Release date:	18 September 2020
Prepared by:	Foresight

*REVISION HISTORY*

Revision	Author	Date	Comments
0.1	Foresight	14 August 2020	Initial draft.
0.2	Foresight	15 August 2020	Updated based on client evidence
1.0	Foresight	24 August 2020	Initial analysis completed.
1.1	Foresight	9 September 2020	Updated with PIR Workshop feedback.
1.2	Foresight	10 September 2020	Draft for peer review.
1.3	Foresight	11 September 2020	Draft for release to client.
1.4	Foresight	15 September 2020	Updated based on client feedback.
1.5	Foresight	17 September 2020	Updated based on client feedback.
1.6	Foresight	18 September 2020	Finalised for release to client.



## Contents

- 1 Executive Summary ..... 4**
- 2 Overview of Incident ..... 7**
  - 2.1 Background..... 7
  - 2.2 Root Cause ..... 7
  - 2.3 Analysis Scope and Process ..... 8
  - 2.4 Report Structure .....10
- 3 Incident Response Approach ..... 11**
  - 3.1 Preparation Phase..... 11
  - 3.2 Detection & Analysis Phase.....13
  - 3.3 Containment Phase .....13
  - 3.4 Eradication Phase .....17
  - 3.5 Recovery Phase.....18
  - 3.6 Lessons Learnt Phase .....19
- 4 Analysis of Incident .....21**
  - 4.1 Preparation Phase.....21
  - 4.2 Detection & Analysis Phase.....21
  - 4.3 Containment Phase .....21
  - 4.4 Eradication Phase .....22
  - 4.5 Recovery Phase.....22
  - 4.6 Lessons Learnt Phase .....23
- 5 Post Incident Recommendations .....26**
  - 5.1 PIR1 – Improve monitoring of the G-Suite environment to detect anomalous behaviour .....26
  - 5.2 PIR2 – Update existing technical processes & design documentation .....26
  - 5.3 PIR3 – Undertake incident tabletop exercises.....27
  - 5.4 PIR4 – Improve existing incident response collaboration and tooling capability .....27
  - 5.5 PIR5 – Review existing support services with Google.....28
  - 5.6 PIR6 – Regularly review G-Suite technical controls.....28

# 1 Executive Summary

ACT Education engaged Foresight Consulting to assess the incident response approach undertaken for the Email Incident that occurred on 14 August 2020 where inappropriate content was shared by students to all ACT public school students (upwards of 50,000 students impacted).

ACT public school students determined that several G-Suite email groups could be emailed, which were grouped by School Year. Some of these emails included inappropriate messages, links to pornographic content and graphic videos. Parents, teachers and school staff were amongst the initial notifiers for this incident as it was escalated to ACT Education. The Incident Management team was stood up by ACT Education, which included resources across ACT Government who worked with stakeholders to establish that synchronised security groups that could be emailed or shared to as the root cause. System access at multiple levels was restricted to prevent further emails and to minimise the exposure of students to inappropriate content. ACT Education provided multiple communications to both internal and external stakeholders including law enforcement and the media as part of its incident response process. ACT Education engaged an independent security assessor on the day of the incident to provide assurance of the approach undertaken to date and to review its containment, eradication and recovery processes.

Foresight Consulting worked with ACT Education to perform an initial analysis on the processes undertaken to manage, contain and remediate the incident. ACT Education's incident response actions were mapped against a standard incident response lifecycle and its phases, consisting of Preparation, Detection & Analysis, Containment, Eradication, Recovery and Lessons Learnt.

Key actions undertaken during the incident were requested or observed by Foresight for assurance purposes, including:

- Confirmation of the incident root cause.
- Establishing whether the incident was a result of external hackers or internal student misuse.
- Stakeholder engagement & communication.
- Review of measures undertaken to contain the incident.
- Review of the G-Suite environment settings to minimise the risk of incident reoccurrence.
- Appropriate collection and storage of evidence and incident documentation
- Evidence of appropriate testing for the purging of inappropriate content and review of approach for the recovery of services.



- Monitoring and alerting process in place post recovery of services to minimise the risk of incident reoccurrence.

A Post Incident Review workshop was held with ACT Education on Friday 4 September 2020 with technical and management stakeholders involved in the incident. Positive aspects of the incident were discussed, whilst lessons learnt were derived to assist with improvements to ACT Education's people, processes and technology.

Based on interviews, controls implemented, testing undertaken, and the Post Incident Review workshop held with ACT Education, the following recommendations are proposed to improve incident response processes and to further minimise the risk of a similar incident reoccurring:

- Update existing Business Continuity Plans (BCP), procedure documents and system design documentation to address similar future incidents whereby complete system shutdowns are required and to ensure system dependencies and limitations are known prior to an incident occurring.
- Review existing support services with Google to ensure that subject matter experts can be coordinated via the use of a Google Incident/Crisis manager or similar role, and to ensure ACT Education inhouse expertise is available by hiring or training staff with appropriate Google Cloud Professional certifications.
- Future tabletop exercises should consider the G-Suite environment and other cloud systems to ensure familiarisation with the processes and capabilities available to contain and mitigate an incident. Specific procedures could be derived from these regular exercises to further strengthen staff training and reduce the time taken in all phases of the incident lifecycle.
- Improve monitoring of the G-Suite email environment to detect anomalous behaviour via logging of email traffic behaviour, improved alerting rules and creating "monitoring" student accounts.
- Regular technical validation of ACT Education's security controls should occur to provide assurance of operational effectiveness. This should include reviewing the controls implemented as part of containing and recovering from this incident.
- ACT Education should uplift and regularly review the ruleset of its existing internal email filtering capability to minimise the risk of inappropriate content being shared between students in the future.

- I Improve existing incident response collaboration and tooling capability by leveraging existing document management repositories, providing technical training to staff of the investigative / incident management tools available across the ACT Education and ACT Government environments and using existing ITIL ticketing systems to track and manage incident related changes and activities.

Recommendation (grouped)	Priority
PIR1 - Improve monitoring of the G-Suite environment to detect anomalous behaviour	High
PIR2 – Update existing technical processes & design documentation	High
PIR3 – Undertake incident tabletop exercises	Medium
PIR4 – Improve existing incident response collaboration and tooling capability	Medium
PIR5 – Review existing support services with Google	Low
PIR6 – Regularly review G-Suite technical controls	Low

## 2 Overview of Incident

### 2.1 Background

On the morning of 14 August 2020, ACT Education experienced an email incident impacting the ACT public school student email service. The content of these emails included inappropriate content sent to all students (around 50,000). As parents and teachers informed and escalated the issue to ACT Education, an incident response team was formed to manage the issue that was classified as “Priority 1 – Major Incident”. Several internal and external stakeholders were informed of the incident status throughout the day. Root cause analysis determined the issue to be due to several synchronised security groups that could be emailed or shared to that have been in the environment since April 2020 due to the implementation of a web filtering capability<sup>1</sup>.

ACT Education undertook containment measures including capturing incident evidence and audit logs for further analysis. Law enforcement was informed of the incident and ongoing technical mitigating controls were performed to restrict access to the G-Suite environment. Once contained, ACT Education continued its investigation, with further mitigating controls, and recovery planning to resume services.

In the afternoon of 14 August 2020, ACT Education engaged Foresight Consulting to assist with providing assurance that ACT Education was undertaking appropriate steps to manage the incident, contain the incident and recover its G-Suite environment to normal operations. At the conclusion of service recovery, Foresight was also engaged to undertake a Post Incident Review workshop and analysis.

### 2.2 Root Cause

In April 2020, changes were made to the ContentKeeper web filtering capability that resulted in students being grouped by year (Kindergarten through to Year 12). These security groups were created in Active Directory to allow for different filtering rules to apply to each student Year

---

<sup>1</sup> This web filtering capability (ContentKeeper) created ACT Education groups for system management that were synchronised to the G-Suite environment, resulting in email groups created with default settings.

group. The Active Directory Identity Access Management (IdAM) tool captured these newly created security groups and synchronised them to the G-Suite cloud environment as groups.

By default, these groups had the ability to be emailed and shared to by all users of the G-Suite environment, including students. This was an unforeseen consequence of the web filtering changes. Key factors that contributed to this root cause include a lack of holistic system design documents and the lack of broader technical staff knowledge of its systems and key integration points which should be reviewed as part of the Change and Release processes, assessing impacts. Key technical documentation and the Change and Release process to maintain these new holistic system design documentation is recommended.

### 2.3 Analysis Scope and Process

Foresight Consulting worked with ACT Education to perform initial analysis of the processes being undertaken to manage, contain and remediate the incident. Direct access to ACT Education systems involved in this incident was not provided for analysis<sup>2</sup>. Foresight's observations are based on email responses, interviews and screen sharing sessions based on information available to ACT Education and ACT ICT staff during the process of containing and remediating the ongoing incident between Friday 14 August 2020 17:04 and Monday 24 August 2020 12:27. Foresight observed planned Eradication and Recovery approaches, with technical observations made of the G-Suite controls implemented.

The scope for this analysis was as follows:

- **Step 1: Preliminary Discovery** – Workshop and follow-up interviews with key ACT Education and ACT ICT personnel to understand the current processes, containment and remediation actions undertaken to date.
- **Step 2: Compare Incident Response Processes and Actions to Industry Best Practice** – Based on the Preliminary Discovery and further follow-up questions and evidence gathering (where available), compare the processes ACT Education undertook during this incident to industry best practice.

---

<sup>2</sup> As required, evidence was provided via screenshots or screensharing sessions with ACT Education staff.

- **Step 3: Analysis and reporting** – Review and analyse findings, including identification of any issues to date, as well as vulnerabilities and control gaps. Foresight Consulting are to provide recommendations for improvement.

Foresight Consulting undertook the following process for this analysis:

- Brief interviews with the ACT Education CIO (Kelly Bartlett) and ACT SSICT staff (Daniel Ruecraft) to determine the scope of the engagement, background of the incident and containment measures undertaken up to the point of engagement with Foresight.
- Review of additional containment and remediation activities planned to be undertaken by ACT Education and SSICT staff between 17:59 and 19:54 Friday 14 August 2020
- Review of ACT Education’s incident chronology spreadsheet, detailing the activities undertaken between Friday 14 August 2020 and Sunday 16 August 2020.
- Response to follow up questions based on ACT Education’s incident chronology spreadsheet, answered by ACT Education CIO (Kelly Bartlett).
- Review of ACT Education’s “Google Restart Options” PowerPoint pack with detailed remediation options for recovering the impacted services.
- Review of recovery and testing approach with ACT Education staff (Murray McKay, Bill Williamson) on Monday 17 August 2020 10:00.
- Review of Phase 2 incident approach with ACT Education staff (Bill Williamson, David Spencer) on Wednesday 19 August 2020 12:00.
- Review of the Google Vault export status along with purging and restore tests of email.
- Review of G-Suite remediation work with ACT Education staff (Bill Williamson) on Thursday 20 August 2020 9:00.
- Review of Phase 2 incident response analysis with ACT Education CIO (Kelly Bartlett) on Friday 21 August 12:00.
- Review of final recovery and testing approach with ACT Education (Bill Williamson) on Monday 24 August 2020 9:30.
- Review of Active Directory Identity and Access Management settings attributed to the root cause of the incident.
- Review of documented restoration steps prior to enabling Gmail services.

- | Post Incident Review workshop with ACT Education and SSICT staff involved with the incident on Friday 4 September 2020 11:00.

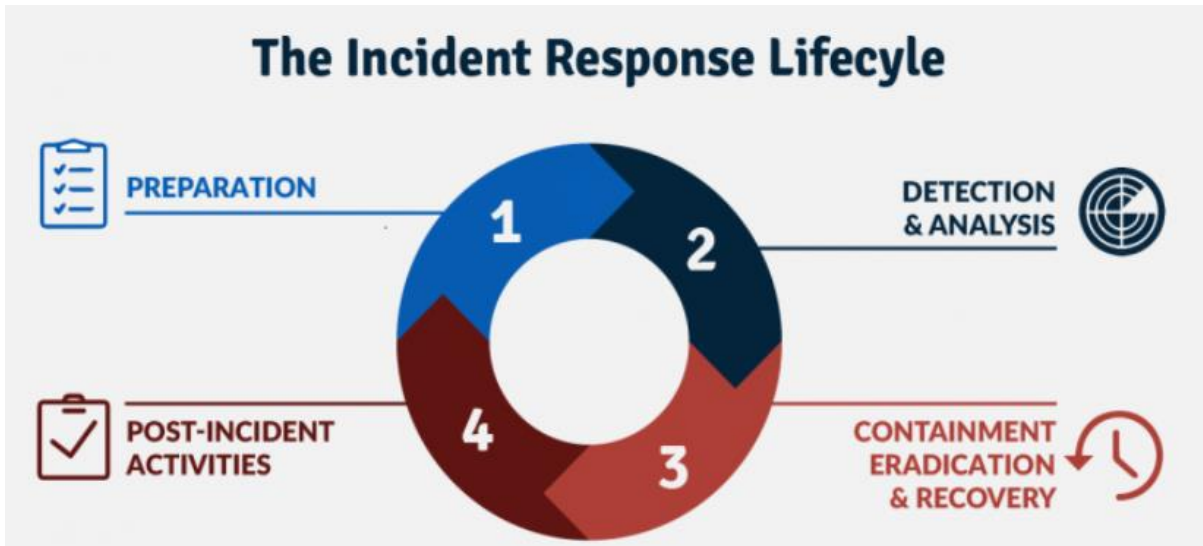
## 2.4 Report Structure

This report contains the following key sections:

- | Executive Summary
- | Overview of Incident
- | Incident Response Approach
- | Analysis of Incident
- | Post Incident Recommendations

### 3 Incident Response Approach

Whilst multiple variations of an incident response lifecycle exist, a majority follow the same principles outlined in the NIST800-61r2 publication "Computer Security Incident Handling Guide".<sup>3</sup> Incident response plans are typically tailored to each organisation, based on their incident handling capabilities and policy requirements. Most modern incident response plans today include the following lifecycle steps:



Incident response should be managed as a lifecycle, whereby stages can be revisited where required if new information comes to life or the incident is dynamic in nature.

#### 3.1 Preparation Phase

The Preparation phase is intended to ensure that organisations have appropriate Incident Response Plans in place, that executive management are involved for communication and decision making purposes and that appropriate staff or outsourcing providers are available to execute these plans in the event an incident is triggered.

##### 3.1.1 Observations

- ACT Education leveraged several internal incident response plans and frameworks including:

---

<sup>3</sup> <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

- Crisis Management Plan (Coordinated by ACT Education Executive, Executive Group Manager, Service Design & Delivery - Ross Hawkins with reporting lines through to the DG Katy Haire and Minister Berry)
- Major IT Incident Process (Coordinated by SSICT – Leon Gerbich/Kylie Blyth & ACT Education CIO – Kelly Bartlett)
- Based on the dynamic nature of the incident, components of ACT Education’s Incident Response Plan were enacted to determine if the incident was related to a potential cyber security breach and if a failure of security controls had occurred.
- The impact of the incident resulted in several ACT Education executives and sections of multi disciplines, impacted stakeholders and third-party suppliers to be involved. This included:
  - ACT Education Executive General Manager, Service Design and Delivery (EGMSDD)
  - ACT Education CIO (Kelly Bartlett)
  - ACT Education – ITO of Chisholm High (Grant Robinson)
  - ACT Education Principal Support (Mark Huxley and DSI’s)
  - ACT Government SSICT Security Operations Directory (Julian Valtas)
  - ACT Education Directorate Digital Strategy, Services and Transformation (DSST)
    - Enterprise Architect (Bill Williamson)
    - Technical Team – Jay Bellchambers, Murray McKay
  - ACT Government Shared Services Information Communications Technology team (SSICT)
    - Including Embedded ICT, Major Incident Management, IDAM, Networks and Security
    - Technical Team - Michael Bayliss , Mark Southwell, Mark Sanderson, Daniel Rucroft
  - ACT Chief Digital Officer
  - Geeks on Tap (ACT Education Google G-Suite Partner)
  - P&C Association
  - AFP Online Child Safety Team
  - ACT Policing
  - ACT Education Media and Comms (Paul Short & Lyn Larkin)
  - ACT Education Governance, Complaints Line (Kaye Yen)
  - ACT Education Complex Student Cases (Sam Seton)



- ACT Education eSafety Officers (Nicole Agius & Kate McMahon)

## 3.2 Detection & Analysis Phase

The detection & analysis phase outlines the triggers for the incident and how the incident was initially raised or discovered. This phase is where incident response teams are stood up and documentation needs to be maintained to document the timeline and evidence discovered as part of the investigation. Communication to various stakeholders is likely to occur based on triaging of the evidence at hand along with the incident prioritisation and impact.

### 3.2.1 Observations

- Initial formal notification of the incident was recorded on 14 August 2020 at 10:59 when an ACT Education staff member (Grant Robinson) informed ACT Education's Digital Strategy, Services and Transformation team to investigate.
- Staff from ACT school Campbell High notified ACT Government SSICT on 14 August 2020 at 11:03 of multiple groups being emailed with inappropriate content.
- ACT Education rated this incident as a Priority 1 – Major Incident on 14 August 2020 at 12:40.
- ACT Education informed its Executive General Manager, Service Design & Delivery (EGMSDD) of a significant ongoing email incident involving multiple ACT public schools on 14 August 2020 at 12:40 which resulted in a request to immediately shut down the Google Platform from the ACT Education CIO.
- No operational or security alerts were generated by ACT Education in response to the email spam activity.
- ACT Education were observed to have documented aspects of the incident including incident chronology (timeline), maintaining integrity of evidence and containment/recovery options.

## 3.3 Containment Phase

In the Containment phase, all impacted assets are identified, and an initial root cause may be established. All relevant audit logs are captured for evidence and future review whilst also being reviewed to determine the extent and impact of the incident across the organisation. Relevant containment/mitigating controls are to be defined and executed as required to minimise further impact. At this point in time, communication to relevant external stakeholders may be required including law enforcement.

### 3.3.1 Observations

- In response to the initial incident triggers, ACT Government SSICT blocked access for users to send to a single group on 14 August 2020 at 11:41.
- Based on further notifications of continued emailing of multiple groups, SSICT investigated the impact of the incident and determined:
  - At least 10 students had leveraged several groups with email and sharing capabilities to send at least 13 initial emails to a large number of other students.
  - These students appear to have also sent emails on behalf of at least six groups.
  - Students initially only emailed one group at time and then eventually determined that “internet-edu-01” through to “internet-edu-12” (groups for each grade of school) could be emailed all at once, impacting all students of the G-Suite platform.
  - Multiple responses and reply all emails were triggered by other students upon receiving the spam. A majority of responses were by students attempting to stop the spam whilst a small minority proceeded with sending inappropriate content.
  - The initial email was determined to be an ACT Year 6 student who accidentally shared a Google Presentation to all ACT Year 8 students.
- At the direction of ACT Education, ACT Government SSICT performed a number of significant containment actions on 14 August 2020 between 12:32 and 13:53:
  - SSICT changed all G-Suite groups starting with “internet” to have a Posting Permission of “Owners Only”.
  - The ACT Education EGMSDD requested for the Gmail service to be shutdown to minimise and contain the incident impact.
  - ACT Education CIO approved SSICT to turn off the Gmail service for students.
  - SSICT recommended the use of the existing ACT Education web filtering solution to assist in blocking weblinks that may contain inappropriate content which was subsequently approved by the ACT Education CIO.
  - ACT Education determined that Active Users could still see emails, with G-Suite services potentially taking up to 24 hours to completely disable access to the environment.

- With approval by the ACT Education CIO, SSICT stopped Google Authentication Services in order to invalidate active user sessions to the G-Suite platform. This initially impacted administrative access to the G-Suite platform however was resolved within 46 minutes.
- SSICT disabled G-Suite access to send to groups.
- ACT Education (the EGMSDD) notified the ACT Chief Digital Officer on 14 August 2020 at 13:40 based on the incident severity and impact to a major ACT Government ICT system.
- ACT Education notified the ACT P&C Association on 14 August 2020 at 14:05.
- ACT Education notified the AFP Online Child Safety Team on 14 August 2020 at 14:30. Email confirmation of the notification was provided back to ACT Education on the same day at 15:52.
- ACT Government SSICT advised the Australian Cyber Security Centre (ACSC) on the day of the incident.
- ACT Government SSICT commenced extraction of the audit logs from key systems involved in the incident on 14 August 2020 at 14:12. The extraction process was initially expected to take between 24-48 hours based on the significant number of user accounts involved (50,000+). Technical issues were encountered that required assistance from Google directly. The Google Vault systems used to place a “hold” on all emails related to the incident and extractions could occur in parallel to ongoing investigations.
- ACT Education School Enterprise Architect confirmed the following additional containment actions had been undertaken on 14 August 2020:
  - The Google Groups service was disabled.
  - The built-in G-Suite investigation tool was leveraged to audit the extent of inappropriate emails.
  - Chromebooks managed by ACT Education were updated to block access to URLs mail.google.com and groups.google.com.
  - Manual suspension of several users was undertaken when it was identified that students were able to create new groups and send emails through cached logons.
  - A custom script was run to determine all non-suspended accounts to determine if email activity was undertaken to subsequently log the event and suspend the account.

- | ACT Education SSICT confirmed the following additional containment actions had been undertaken on 14 August 2020:
  - o Super user access to the G-Suite environment was provided to relevant incident stakeholders to assist in the containment efforts.
  - o Updated the configuration of Google Groups that enabled broad email and sharing functionality via groups.
  - o Leveraged the existing ACT Education web filter to block access to Google Mail domains via wired/wireless ACT public school networks.
  - o Google Single Sign on integration was disabled.
- | ACT Education coordinated with Geeks on Tap on 14 August 2020 between 14:39 and 15:25 to undertake several containment actions including:
  - o Disabled access for all Managed Devices (Google Chromebooks).
  - o Restricted access to G-Suite to restricted IP addresses used by ACT Education for administration.
  - o Turned off all Android, iOS and Google Sync services that would have allowed continued access to G-Suite emails.
- | All remaining G-suite users were confirmed to be suspended, with the incident considered to be contained on 14 August 2020 at 20:42.
- | ACT Policing contact ACT Education via the EGMSDD to discuss the ongoing incident on 15 August 2020 at 11:30. An onsite meeting was held between ACT Policing and ACT Education stakeholders on the same day at 12:30 with the following outcomes:
  - o ACT Policing will commence a review/investigation into the incident.
  - o ACT Policing will also support ACT school principals with appropriate discussions.
- | ACT Education Media and Comms staff (Lyn Larkin) engaged with the media to provide an update of the incident on 14 August 2020 at 19:00. The following media articles were observed on the initial day of the incident:
  - o The Canberra Times "ACT school students' emails inundated with inappropriate material" at 16:00.
  - o iTnews.com.au "ACT Education blocks student Gmail access after spam email storm" at 17:05.

- ABC News "Canberra students gained access to school network to send graphic content to children across ACT" at 21:11.

### 3.4 Eradication Phase

The Eradication phase is intent on preserving all incident artefacts for any future investigations required but also to begin purging these artefacts from the environment to assist in the recovery to normal operations. The root cause of the incident should be clearly identified and fully understood at this stage to assist in both short term and long-term mitigating controls.

#### 3.4.1 Observations

- In identifying the root cause of the incident, ACT Education have determined that the affected groups allowing students to send emails (prefixed with "internet") were created due to a system change on 28/04/2020. This system change was in relation to ACT Education's web filtering solution (Content Keeper), which is connected to ACT Education's Active Directory instance via Active Directory IDAM synchronisation. Changes to School based rules to Year based rules (in alignment with Australian Curriculum) inadvertently resulted in these new groups being synchronised to the Google S-Suite environment. Default G-Suite permission settings were applied which allows anyone to post messages to the groups.
- Further investigation into the permissions of all other groups setup in the G-Suite environment was undertaken. ACT Education did not observe any other groups setup in a way that would allow students to email other unintended groups.
- ACT Education elected to instead delete all groups containing students as further testing found that sharing of content could still occur via Google Drives and other collaboration methods.
- Removal of all inappropriate emails took place prior to the planned G-Suite email reactivation date of 24 August 2020.
- ACT Education worked with Google directly to ensure copies of all email messages during the incident period are maintained prior to removal. This was to assist with further incident investigation from various internal and external stakeholders (including law enforcement).
- ACT Education have setup an appropriate evidence storage environment that will be leveraged for future investigations and long-term archiving of evidence data.

- Removal of emails sent from 10am onwards on the day of the incident has been undertaken to purge all instances of inappropriate content. Legitimate student emails from the day can be recovered upon request. ACT Education undertook testing to validate this approach.

### 3.5 Recovery Phase

The Recovery phase is to restore the impacted environment to normal operations. All systems are to be brought back to their original state prior to the incident and all appropriate mitigating controls should be implemented at this stage to prevent a reoccurrence of the incident.

#### 3.5.1 Observations

ACT Education planned to execute the recovery in two major phases. Prior to commencing with Phase One, the following activities were undertaken by ACT Education:

- Assurance from an independent security assessor that ACT Education have undertaken appropriate incident response measures.
- Proposed changes to the G-Suite collaboration settings were agreed by ACT Education stakeholders.
- A testing program was used to replicate student activity to ensure appropriate security controls were in place to prevent an incident reoccurrence.
  - Testing outcomes were shared with SSICT, Google and an independent security assessor for review.

#### Phase One – Reactivation of access to the G-Suite environment (minus Gmail):

- ACT Education undertook an extensive review and uplift of its collaboration settings in the G-Suite environment to ensure removal of student access to global groups.
- G-Suite services (excluding Gmail) were activated with settings modified to restrict students from emailing or sharing to groups.
- The following baseline system changes were implemented across the environment:
  - Students are unable to create groups that could be used as future groups.
  - Students are unable to post or share content to groups.
  - All student created groups were disabled.

## Phase Two – Reactivation of access to Gmail:

- | ACT Education resumed Gmail services on 24 August 2020.
- | Prior to enabling access to Gmail, the following ACT Education prerequisites were performed:
  - o Copy of all email messages and audit logs as part of the incident investigation was exported.
  - o ACT Education and SSICT continued reviewing and assessing student activity.
  - o Purge of all emails from 10am onwards on the day of the incident.
  - o Undertook a review of the Phase Two approach and testing outcomes of Phase One with SSICT, Google and an independent security assessor.
  - o Notification to the AFP of ACT Education activities undertaken to assist with finalisation of AFP's investigation into the incident.
  - o ACT Education have undertaken manual verification of any remaining emails from the day of the incident in student inboxes. This was to further minimise the risk of residual inappropriate content that may have been missed from the global purge job.
  - o Manual monitoring was put in place by ACT Education staff to observe and minimise the risk of incident reoccurrence. ACT Education are considering a long-term monitoring solution for the environment.
- | Gmail services were successfully recovered on the evening of Monday 24 August 2020. No evidence of incident reoccurrence has been observed in the environment.

## 3.6 Lessons Learnt Phase

The Lessons Learnt phase is to perform a Post Incident Review (PIR) process in order to address long term mitigating controls that would ensure that reoccurrences of the same or similar incidents do not occur, but to also determine any improvements to the process, people or technology involved in the incident response actions.

### 3.6.1 Observations

- | ACT Education engaged an independent security assessor to undertake a comprehensive review of the incident to determine:

- Validate whether ACT Education has understood the root cause analysis of the incident and whether appropriate mitigation has been undertaken.
- Whether the incident response approach and actions undertaken by ACT Education and SSICT were appropriate.
- What further actions are recommended to ensure a similar breach will not occur again.
- A Post Incident Review (PIR) workshop was held with ACT Education and ACT SSICT stakeholders involved in the incident on Friday 4 September 2020 at 11:00 to:
  - Derive lessons learnt from the emailing incident.
  - Determine improvements in ACT Education's people, processes & technology to minimise the risk of incident reoccurrence and impact.
  - Document the observations, lessons learnt and recommendations.



## 4 Analysis of Incident

This section of the report outlines Foresight's assessment of ACT Education's incident response approach and post incident analysis. An overview of each incident response phase has been provided highlighting both positive observations and areas for improvement.

### 4.1 Preparation Phase

#### 4.1.1 Positive observations

ACT Education had established incident response plans and adequate staff who were aware of their roles and responsibilities during the incident.

#### 4.1.2 Areas for improvement

- Whilst ACT Education and SSICT staff managed the incident appropriately, staff had not previously experienced an incident of this scale or public visibility.

### 4.2 Detection & Analysis Phase

#### 4.2.1 Positive observations

Given the length of time (57 minutes) between the first emails occurring between students and escalation to ACT Education, the approach taken was appropriate. Communication to stakeholders and ACT Education executives was considered and actioned, with multiple levels of incident response teams activated to manage the incident appropriately.

#### 4.2.2 Areas for improvement

- ACT Education monitoring systems (both operational and security) did not detect the unusual group activity occurring nor the inappropriate content being distributed internally within the G-Suite environment.
- The existing internal email content filter could be regularly reviewed, with uplifting of the ruleset as required to improve the detection of inappropriate email and content being distributed amongst students.

### 4.3 Containment Phase

#### 4.3.1 Positive observations

ACT Education's approach to containing the incident was appropriate given the dynamic nature of the incident. SSICT addressed each identified group however additional incident triggers required an escalation in response. With appropriate executive level approval, ACT Education systematically

removed or disabled the ability for students to continue emailing inappropriate content. Within two hours, ACT Education had disabled Gmail services and addressed ongoing access to the platform via disabling other Google services whilst investigating the root cause and impact of the incident.

#### 4.3.2 Areas for improvement

- Future tabletop exercises should be considered that involve the ACT Education environment to ensure familiarisation with the processes and capabilities available to contain and mitigate an incident. Specific procedures could be derived from these regular exercises to further strengthen staff training and reduce the amount of time taken in all phases of the incident lifecycle.

### 4.4 Eradication Phase

#### 4.4.1 Positive observations

Root cause analysis was appropriately undertaken by ACT Education and determined that the groups used in the emailing of students were created as part of a system change in April 2020. Further investigations by ACT Education found no other groups that could be abused by students based on misconfigured permissions.

Prior to reactivating the service, ACT Education will be purging all identified inappropriate content from student email accounts. However, the exact technical methods being undertaken by ACT Education were not provided for this analysis.

#### 4.4.2 Areas for improvement

- SSICT's technical playbook for exporting data from G-Suite did not work at the time due to issues with the tooling and the sheer size of the data export being undertaken.
- Purging of all emails from the day of the incident required Google assistance due to the size of the job and issues with tooling.

### 4.5 Recovery Phase

#### 4.5.1 Positive observations

ACT Education considered a balanced approach to restore access to the G-Suite environment in a manner that minimises ongoing disruption to ACT public school students but also allows for ACT Education technical staff to thoroughly test and plan the resumption of Gmail services to all students. Several settings are expected to be modified to restrict the ability for groups to be

abused but also other sharing mechanisms that could be potentially abused such as Shared Drives. ACT Education are also engaging with their stakeholders and external partners to review the test results of its Phase One service resumption.

#### 4.5.2 Areas for improvement

- Whilst manual log monitoring was in place for the Recovery phase, automated log monitoring and use cases should be investigated to provide early warning of future attempts to abuse the G-Suite environment.

## 4.6 Lessons Learnt Phase

### 4.6.1 Positive Observations

- A Post Incident Review (PIR) was undertaken by ACT Education to determine if improvements can be made to the people, process and technology involved in the incident. This was also to minimise the risk of future similar incidents occurring to the same extent and impact.
- ACT Education's communications management to all internal and external stakeholders was appropriate, ensuring timely updates and regular engagement occurred throughout the incident.
- ACT Education ensured that misattribution of the incident root cause did not occur, particularly to rule out any malicious attacker activity.
- Staff involved in the incident managed a dynamic situation well and adapted accordingly to the external pressures involved with a publicly visible and media covered incident.
- Collaboration between ACT Education and SSICT technical staff was noted to be excellent with both parties undertaking significant out of hours assistance.
- ACT Education and SSICT technical staff developed scripts to assist with issues encountered with the tooling available as a result of both the large amount of emails involved along with configuring settings at scale.
- The time taken to detect and analyse the incident was considered to be appropriate.
- The use of Microsoft Teams as the primary incident response communication tool allowed for the recording of stakeholder communication as well as broader distribution of information to both technical and management stakeholders. ACT Education management stakeholders for example were directly available to technical staff which provided for clear communication and quicker decision making.

- | A majority of students responded in an appropriate manner during the incident. Some students assisted by marking inappropriate email as spam, causing a number of students to be banned from sending further emails.
- | Whilst ACT Education appropriately contained the incident by rectifying the misconfiguration of various groups, additional testing by staff found that misuse via other G-Suite services was possible and the groups were removed from the environment once they were deemed to be not required for any system functions.
- | ACT Education Senior Executives were involved early in the incident and undertook quick decision making which minimised delays in containment.
- | Support from ACT Education Senior Executives, other branches and the Minister was deemed to be excellent by ACT Education staff during the incident.
- | Active monitoring and use case tests were undertaken during the Containment and Eradication phases, with ACT Education covering multiple use cases to minimise incident reoccurrence.
- | An appropriate evidence collection and storing methodology was established to capture all artefacts related to the incident for long term storage and use by ACT Policing and the AFP in any future investigations.
- | External partners such as Geeks on Tap and Google provided adequate assistance during the incident.
- | Recovery of the G-Suite environment was not rushed, with ACT Education ensuring that all inappropriate material was removed from the environment prior to recovery of services.

#### 4.6.2 Areas for improvement

- | Previously documented BCP plans and technical documentation did not factor in a student misuse scenario. ACT Education and SSICT had to adapt their approach to the incident to accommodate for this.
- | The existing security assessments undertaken against ACT Education's G-Suite environment is unlikely to have detected the root cause of this incident as it was an unintended system side effect.
- | Broader system diagrams and documentation (including applications, integration and networks) is required to improve the assessment and review of the environment (e.g. holistic ecosystem diagrams) when it comes to troubleshooting incidents. This could also include

system RACIs to clearly define which groups in ACT Education and SSICT are responsible for particular system components.

- | Some collaboration improvements could be made to the incident and evidence gathering process including additional training and use of existing investigative tools, managing and tracking incidents, and centralising the incident documentation for all stakeholders involved. This may involve the shared use of systems across both ACT Education and SSICT.
- | ACT Education's existing monitoring systems of the G-Suite environment could be improved upon to detect future occurrences of unusual email traffic in a short period of time.
- | The use of monitoring G-Suite accounts emulating a student could be used to improve the detection of similar future incidents. ACT Education staff were reliant on using the accounts of their own children during the incident (to perform testing and validation).
- | Both ACT Education and SSICT technical procedures need to be updated to reflect shutdown of services based on student misuse, rather than as a Business Continuity Plan. Several technical issues were identified in the shutdown process that had to be addressed adhoc by staff and external partners such as Geeks on Tap and Google.
- | Whilst Google provided adequate "consumer support", a dedicated Google Major Crisis/Incident response coordinator could have assisted with addressing the technical issues observed in the environment during the Containment and Eradication phases.
- | Regular technical validation of ACT Education's G-Suite security controls should be considered to provide assurance of effectiveness. This should include reviewing the controls implemented as part of containing and recovering from this incident.

## 5 Post Incident Recommendations

The following recommendations have been derived from Foresight's assessment of areas for improvement with ACT Education's incident response approach and post incident analysis.

### 5.1 PIR1 – Improve monitoring of the G-Suite environment to detect anomalous behaviour

**Priority: High**

Monitoring of the G-Suite environment should be improved to detect future instances of anomalous behaviour. This could include:

- Automated log monitoring to alert on significant increases in email traffic in a short period of time.
- Use of "monitoring" email accounts in the student G-Suite environment, designed for use by ACT Education as early warning of service misuse.

### 5.2 PIR2 – Update existing technical processes & design documentation

**Priority: High**

- All G-Suite system documentation should be updated to improve ongoing maintenance and assist in future incidents by including:
  - Complete ecosystem diagrams showing the integration points of related systems (e.g. how changes to the web filtering system and Active Directory would affect G-Suite).
  - Documentation of all applications, integrations and networks for the G-Suite environment (including on premise systems)
  - RACIs derived for each component of the G-Suite environment to clearly outline the responsibilities for each ACT Education and SSICT sections.
  - Ensure ongoing Change and Release processes include the updating of system documentation and diagrams by change owners and technical implementation staff to aid with future management and incident handling.
- Existing ACT Education technical processes should be updated to consider system shutdowns as a likely containment measure in the event of an incident. The processes involved in the "shutdown" of a cloud-based environment are complex when compared to an on-premise solution. Documenting the caveats and dependencies would assist in staff readiness.

### 5.3 PIR3 – Undertake incident tabletop exercises

Priority: **Medium**

Regular tabletop exercises should be undertaken by ACT Education to improve staff awareness of their roles and processes during an incident. This can result in improvements to existing processes and forcing documentation to be current and relevant. Tabletop exercises are paper based and involve simulating a scenario that can involve both technical and management stakeholders. ACT Education should look at implementing this on a yearly basis and increasing it to every six months once the process is established and understood.

### 5.4 PIR4 – Improve existing incident response collaboration and tooling capability

Priority: **Medium**

Several improvements could be made to ACT Education's incident response collaboration and tooling:

- Centralising active incident documentation (including logs, timelines and evidence) into ACT Education's existing document repository. SSICT should have access to this repository during shared incidents/investigations to minimise the risk of double handling of information. This will aid in collaboration, version history and auditing.
- Additional training and documentation may be required to uplift both ACT Education and SSICT staff knowledge and skills in the use of existing investigative tools such as Google Vault. This would instil confidence into the tools and process without the risk of "learning on the job" in a future incident.
- Whilst the use of Microsoft Teams for incident communication was praised by both ACT Education and SSICT staff, a centralised incident management capability, such as those built into existing ITIL type ticketing systems could be leveraged to track individual tasks assigned to sections. SSICT currently manage the ticketing system used in this incident which ACT Education could have also leveraged. This would aid in the incident documentation process as well as provide evidence of approved changes undertaken to systems during containment and eradication post incident.

## 5.5 PIR5 – Review existing support services with Google

Priority: **Low**

- ACT Education should consider establishing with Google directly, the concept of a Major Incident/Crisis manager to leverage in the event of an incident involving the G-Suite environment. Given the scale of the ACT Education environment compared to corporate environments, access to subject matter experts and coordination of Google support resources may be required in future incidents.
- In addition, ACT Education may consider onboarding or train inhouse Google Cloud Certified Professionals (with Google Cloud Security Engineer or Cloud Architect certifications) to assist with maintaining and supporting the G-Suite environment.

## 5.6 PIR6 – Regularly review G-Suite technical controls

Priority: **Low**

- For ongoing assurance, ACT Education should consider conducting technical reviews of all controls implemented as part of this incident to ensure that they remain effective. This could include reviewing every six months, the settings and composition of groups, collaboration settings for G-Suite and effectiveness of the web filtering solution.
- In addition, security assessments of ACT Education systems involving students as the userbase should not only include students as potential hacking actors but also as abusers of system components and configuration as a means of disruption.
- Regular review and uplift of the existing internal email filtering solution and its ruleset to detect and prevent students sending inappropriate content to other recipients.



End of document.



Trim No. MIN20/1411

## Caveat Brief

**To:** Minister for Education and Early Childhood Development  
**From:** Katy Haire, Director-General Education Directorate  
**Subject:** Email incident update – ACT Policing Investigation  
**Date:** 2 October 2020

That you note this update about the email incident which occurred on 14 August 2020.



Noted / Please discuss

Yvette Berry MLA 16/10/20

- On 14 August 2020, an email incident occurred across the ACT public school Google platform resulting in the distribution of group emails (including some containing inappropriate material) to students using their Gmail accounts on the Google Suite for Education.
- The Education Directorate limited user access to the Google Suite for Education (GSFE) including email and the Google platform. Access to the GSFE was restored in two phases: GSFE access was reactivated Monday 17 August 2020, and Gmail was made reactivated on Monday 24 August 2020.
- The Directorate contacted the Australian Federal Police (ACT Policing), the ACT Chief Digital Officer and the eSafety Commissioner on 14 August 2020 immediately after being notified of the incident and after restricting access to the platform.
- The Directorate advised ACT Policing of the incident and provided information relating to the emails and the material that was shared across the email platform.
- An investigation was commenced by ACT Policing into the distribution of explicit material over the ACT student Gmail platform. The police investigation identified [redacted] students that sent content that could be perceived as explicit in content.
- [redacted] students participated in interviews with ACT Policing and all students were remorseful for their actions. The [redacted] student declined to interview, however has expressed remorse for their actions.
- All students have stated that they are willing to engage in ongoing counselling to assist in rectifying their behaviour.
- ACT Policing have advised that based on this information, their investigation is concluded, and the matter will finalised. No criminal charges will be laid in the matter.

Signatory Name: Katy Haire  
 Title: Director-General, ACT Education Directorate  
 Date: 2 October 2020



Ms Bettina Konti  
Chief Digital Officer  
Chief Minister, Treasury and Economic Development Directorate  
[CDO@act.gov.au](mailto:CDO@act.gov.au)

Dear Ms Konti

Thank you for your support in addressing the PriceWaterhouseCoopers (PwC) Gmail Incident Process Control Review.

As you are aware, on 14 August 2020, the Directorate identified an incident involving unauthorised use of group distribution lists within the Google for Education platform by students which exposed students to inappropriate content.

A change to the web filtering system (ContentKeeper) required new Active Directory security groups, the Identity and Access Management systems copied those groups and published them into the Google for Education platform which resulted in the creation of year group distribution lists, which a student accidentally discovered. With this unintended capability having been exposed, there was a cascading series of emails sent by other students across a variety of group email lists that covered entire year groups across the ACT public school education system.

The key recommendations in which we require ongoing support and improvements include:

1. Improvements to the Change Management processes to prevent unintended issues from affecting supporting or connected systems
2. Agreement to the Managed Service of the Google for Education and Microsoft platforms
3. Improvements and support for Major Incident Management

I understand that you attend the Google and Microsoft Managed Service Steering Committee to ensure that agreement is made. I would appreciate it if you also monitor the improvements of Change Management and Major Incident Management in that forum.

The Google for Education platform was implemented in 2016 under the ACT Education funded Learn Anywhere Program delivered by SSICT and forms an important part to students' learning journey in the ACT. The Google for Education platform has not only supported students, particularly secondary students through

their blended learning journey, but also was a fantastic tool to support ACT students through the Remote Learning period in 2020.

The ACT Education Directorate will continue to partner with the eSafety Commissioner and the Australian Federal Police to deliver eSafety support and resources that provides teachers, students and their carers with accessible information and tools that further enable them to be responsible and engaged digital citizens.

My team will also continue to work closely with your team to ensure the digital platform continues to support children and young people on their learning journey, in a safe environment.

I acknowledge that occasional issues may be encountered with these processes and the continuing improvements to ACT Education systems. In these instances, it is critical that we are able to access ongoing support and connection from your team. Your commitment to the provision of this support is greatly appreciated.

I look forward to continuing working collaboratively with your team and to further strengthening these valuable cross-directorate relationships.

Please contact Kate McMahon, Executive Group Manager Service Design and Delivery ([Kate.Mcmahon@act.gov.au](mailto:Kate.Mcmahon@act.gov.au)) as needed.

Yours sincerely



Katy Haire  
Director-General  
ACT Education Directorate  
26 July 2021



## Caveat Brief



**To:** Minister for Education and Youth Affairs  
**Subject:** Gmail Post Incident Review – Independent Audit outcomes and progress  
**Date:** 9 July 2021

That you note:

- 1) the independent audit report conducted by PriceWaterhouseCoopers (PwC) regarding the Gmail incident of 14 August 2020;

**Noted / Please Discuss**

- 2) the independent audit report was presented to ACT Educations Audit Committee (Attachment A); and

**Noted / Please Discuss**

- 3) the progress made to date against the independent audit reports recommendations.

**Noted / Please Discuss**

Yvette Berry MLA

... 28/07/21

Minister's Office Feedback

- On 14 August 2020, an email incident occurred across the ACT public school Google platform, resulting in the distribution of group emails (including some containing inappropriate material) to students.
- On the same day, you requested the Directorate obtain an independent audit of the incident to determine its root cause and to provide assurance the incident could not be repeated.
- On 10 September 2020, you endorsed the Terms of Reference for the independent audit.
- The Directorate engaged its audit partner, PriceWaterhouseCoopers (PwC), to perform a post incident review. PwC was selected for their audit, assurance and cyber security expertise.
- The PwC final report on the Gmail Incident Process Control Review (final report) was received 28 April 2021 and is at Attachment A.

- The final report was presented to the ACT Education Audit Committee 22 June 2021.
- The final report provided a clear understanding of the root cause and the management and control of the Google system, including the role of Shared Services ICT (now known as Digital Data and Technology Solutions [DDTS]). The final report detailed recommendations to reduce the risk of a repeat incident.
- All actions arising from the final report recommendations have been completed or are underway.
- The Directorate has engaged DDTS to formalise support, including updating documented design and agreement and documentation of roles, responsibilities and service expectations. This body of work is being monitored through fortnightly meetings with the ACT Chief Digital Officer.
- Full implementation of agreed actions is expected to be achieved by 31 December 2021.

Signatory Name: Katy Haire  
Title Director-General  
Date 12 July 2021





# Gmail Incident Process Control Review

## Final report

28 April 2021

### Disclaimer

This internal audit report has been prepared by PricewaterhouseCoopers (PwC) in accordance with the terms of Work Order Number EDU20/1504 dated 17 September 2020. This report is solely for the information of the ACT Education Directorate. Its existence may not be disclosed nor its contents published in any way without the prior written approval of PwC. PwC does not accept any responsibility to any other party to whom this Terms of Reference may be shown or into whose hands it may come.

Whilst the work performed may involve the analysis of financial information and accounting records, it does not constitute an audit or review in accordance with Australian Auditing Standards, Standards on Review Engagements or Standards on Assurance Engagements as issued by the Auditing and Assurance Standards Board and accordingly no such assurance will be provided in any of our deliverables.

## Table of Contents

1. Executive summary.....	1
2. Review overview .....	3
2.1 Review objectives and criteria.....	3
2.2 Methodology.....	3
3. Assessment against scope criteria .....	4
4. Detailed findings and recommendations.....	7
4.1 Governance accountabilities and responsibilities.....	7
4.2 Guidance and security standards .....	9
4.3 System design documentation.....	10
4.4 Monitoring over G-suite configuration and usage.....	12
4.5 Ongoing communication to students and parents/guardians.....	13
5. Recommendations and management response.....	14
Appendix A – Key Control Considerations for Managing/Configuring G-Suite .....	18
Appendix B – Foresight Consulting Review.....	19
Appendix C – RACI recommendation.....	20
Appendix D – Directorate risk matrix .....	21
Appendix E – Stakeholder consultations .....	23
Appendix F – Key Documentation Reviewed .....	24



## 1. Executive summary

### Background

In August 2020, the Directorate identified an incident involving unauthorised use of group distribution lists within the Google for Education platform by students which exposed students to inappropriate content. A change to the web filtering system (ContentKeeper) required new Active Directory security groups, the Identity and Access Management systems copied those groups and published them into the Google for Education platform which resulted in the creation of year group distribution lists, which a student accidentally discovered. With this unintended capability having been exposed, there was a cascading series of emails sent by other students across a variety of group email lists that covered entire year groups across the ACT public school education system. This occurred through the Education Directorate's deployment of Gmail for student email.

As a result, the Directorate engaged PwC to conduct an independent review of the Directorate's management processes for Gmail. In particular, the objectives of this post incident review were to:

- Assess the adequacy of governance arrangements in place between the Directorate and Shared Services ICT (SSICT) with respect to administration and response to critical events. This included a focus on the clarity of roles, responsibilities and escalation channels;
- Provide a root cause analysis of the incident, defining what took place, the impacting factors and providing recommendations to ensure a similar incident does not take place again; and
- Evaluate the incident response in terms of appropriateness and timeliness of actions by both the Directorate and SSICT.

Fieldwork was undertaken from 28 September 2020 – 6 November 2020. Findings and recommendations in this report are reflective of the Directorate's position as at the completion of fieldwork.

### Conclusion

The Directorate is progressing initiatives aimed at improving governance over the G-suite system. This includes addressing weaknesses highlighted in this report and updating existing procedures to prevent a recurrence.

The Directorate and SSICT were able to promptly coordinate and mobilise to address the incident, despite not developing a specific incident response plan for the event. Work is also underway to formalise the service scope between the Directorate and SSICT to provide clarity on the responsibilities of each party.

As a priority the Directorate should:

- Formalise roles and responsibilities related to the management of the G-suite system between teams within the Directorate and SSICT;
- Establish guidance and security standards for the proper management of the G-suite system based on the current end-users (i.e. students);
- Maintain up-to-date enterprise wide system design documentation to improve the efficiency of IT operations and effectively identify emerging risks from planned updates to the system and integrated applications or services; and
- Establish regular reporting of monitoring results and exceptions to the Directorate to improve governance oversight.

Other opportunities for the Directorate to strengthen management of the G-suite system include:

- Regular communication of the Acceptable Use Policy to parents/guardians and end-users to assist in avoiding system misuse; and
- Adoption of additional controls as part of the G-suite system management uplift as outlined at [Appendix A](#).

## 2. Review overview

### 2.1 Review objectives and criteria

The objective of this review was to provide assurance to the Director-General, Senior Executive and the Audit Committee over:

- Adequacy of governance arrangements in place between the Directorate and SSICT, with respect to administration and response to critical events. This included a focus on the clarity of roles, responsibilities and escalation channels;
- Adequacy of process controls, including a root cause analysis of the incident, defining what took place, the impacting factors and providing recommendations to ensure a similar incident does not take place again; and
- Appropriateness of incident response, in terms of timeliness of actions by both the Directorate and SSICT.

### 2.2 Methodology

The review was undertaken by PricewaterhouseCoopers (as an approved ACT Panel Service provider). The Directorate's IT team were also involved from a planning and quality assurance perspective. Fieldwork was undertaken from 28 September 2020 – 6 November 2020.

The methodology for the review included:

- Entry meetings with relevant executive and management to introduce the review team, discuss the review approach, timing and obtain key contacts for the review;
- Obtaining relevant documentation including the report prepared by Foresight Consulting (refer [Appendix B](#)), the Directorate's internal reviews, G-suite documentation and relevant policies, procedures, and guidelines;
- Reviewing documentation and conducting an assessment of action undertaken by the Directorate and SSICT;
- Meeting with relevant executive and management to understand and assess scope items as required;
- Interviews with the relevant IT teams to assess implementation and understanding of current processes, along with areas in which teams would welcome additional support and guidance;
- Preparation of draft findings and meeting with relevant Directorate executive and management to discuss draft findings;
- Preparation of a formal draft report, including quality assurance of findings by PwC and the Directorate;
- Meeting with relevant Directorate management and executive to discuss the draft report;
- Amending the draft report (as necessary to incorporate management feedback) and circulating the draft report for formal management comments; and
- Receipt of management comments and report finalisation.

### 3. Assessment against scope criteria

The table below provides a summary of positive observations, findings and recommendations against the review scope criteria. Detailed findings and recommendations are provided in [Section 4](#).

Audit Criteria	Summary of positive observations and key findings	Summary of recommendations
Adequacy of governance arrangements in place between the Directorate and SSICT	<p><b>Positive observations</b></p> <ul style="list-style-type: none"> <li>The Directorate is analysing the requirements for formalising the service scope between the Directorate and SSICT to provide clarity on the responsibilities of each party.</li> </ul> <p><b>Findings</b></p> <p><i>High Risk</i> (refer to <a href="#">Section 4.1</a>)</p> <ul style="list-style-type: none"> <li>There is currently no formal service level agreement between the Directorate and SSICT which outlines the roles and responsibilities of the support teams for the different components and management elements of the system.</li> </ul>	<p>1. The Directorate should continue to engage with SSICT to clarify and document roles and responsibilities associated with management of the G-suite system. Regular compliance reviews should be performed to:</p> <ol style="list-style-type: none"> <li>maintain adherence to agreed roles and responsibilities;</li> <li>provide an opportunity to re-educate the Directorate and SSICT teams on their roles and responsibilities; and</li> <li>provide an opportunity to re-assess and improve team accountabilities based on the current use, structure, and management capabilities of the G-Suite system.</li> </ol>
Adequacy of process controls	<p><b>Positive observations</b></p> <ul style="list-style-type: none"> <li>The Directorate is progressing initiatives aimed at addressing weaknesses highlighted by the incident. These improvement initiatives relate to management of the system and overall effectiveness of existing incident management processes.</li> </ul> <p><b>Findings</b></p> <p><i>Medium Risk</i> (refer to <a href="#">Section 4.2</a>, <a href="#">Section 4.3</a>, <a href="#">Section 4.4</a>)</p> <ul style="list-style-type: none"> <li>Stringent security standards from either SSICT or the Directorate cannot be fully applied due to the ease-of-use requirements of the system's end-users (students).</li> <li>The Change Management process did not assess the technical impact of the ContentKeeper changes.</li> <li>Several deficiencies were identified with respect to the G-suite system design documentation, including: <ul style="list-style-type: none"> <li>Documentation has not been updated since 2014 and does not reflect the current state of the system.</li> </ul> </li> </ul>	<p>2. The Directorate should:</p> <ol style="list-style-type: none"> <li>establish specific governance and security control standards appropriate to SSICT, the Directorate and end-users of the G-suite system. There is a G-suite security checklist that can be used as a base to establish the necessary built-in configuration items. These items will need to be customised to align with the Directorate's acceptable risk appetite;</li> <li>work closely with the vendor to provide regular training and support for the teams managing the system to progressively improve in-house capabilities.</li> </ol> <p>3. The Directorate should:</p> <ol style="list-style-type: none"> <li>update the current design documentation to address the weaknesses observed; and</li> <li>consider integrating a design documentation update process with change and incident management processes to ensure records are kept up to date and consequently improve the overall effectiveness of IT operations.</li> </ol>

Audit Criteria	Summary of positive observations and key findings	Summary of recommendations
	<ul style="list-style-type: none"> <li>○ The documentation does not include, or refer to, any integration mapping details for related systems.</li> <li>○ Security considerations and mitigating controls for application features are not specifically highlighted to address the application's specific use-case (i.e. end-users are minors).</li> <li>○ Roles and responsibilities for managing the system post implementation between the Directorate and SSICT teams are not defined.</li> <li>● Monitoring procedures do not include monitoring of anomalous usage due to limitations on data that can be accessed and traditional automated security tools cannot be utilised.</li> </ul>	<ul style="list-style-type: none"> <li>c. Review and update the Change Management process, of all systems to consider the impact of other integrated or connected systems.</li> </ul> <p>4. The Directorate should continue to engage with SSICT to ensure regular reporting of monitoring results and exceptions is performed by SSICT and submitted to the Directorate for review. The Directorate should review any exceptions reported in terms of compliance with approved policies and procedures. Exceptions should also be assessed as to whether they represent possible weaknesses in current system and management controls for the G-Suite system.</p> <p>In the interim (while more robust monitoring processes are being developed), SSICT and the Directorate should maximise the use of existing features within the application to support improved monitoring of the application. For example:</p> <ul style="list-style-type: none"> <li>● Data from G-Suite Highlights report could be used to perform further analysis to identify indicators of anomalous usage of features within the application; and</li> <li>● Dummy accounts could be set up to detect similar incidents and monitor what is publicly distributed within the application.</li> </ul>
Appropriateness of incident response	<p><b>Positive observations</b></p> <ul style="list-style-type: none"> <li>● Based on stakeholder consultations and the report provided by Foresight Consulting, the Directorate promptly coordinate and mobilise to address the incident, despite not developing a specific incident response plan for the event.</li> </ul> <p><b>Findings</b></p> <p><i>Low Risk</i></p> <ul style="list-style-type: none"> <li>● The standard WhoG Major Incident process was not adopted</li> </ul>	<p>5. The Directorate should continue to engage with SSICT Major Incident process to ensure triaging process, including notification and expert advice be sought from the Directorate.</p>

Audit Criteria	Summary of positive observations and key findings	Summary of recommendations
Opportunities to further strengthen current processes	<p><b>Findings</b></p> <p><i>Low Risk</i> (refer to <a href="#">Section 4.5</a>)</p> <ul style="list-style-type: none"> <li>As end-users are primarily comprised of minors, parents/guardians can be engaged to help support initiatives aimed at promoting acceptable behaviour when using the G-suite system.</li> </ul>	<p>6. Guidance on acceptable use of the system should be regularly communicated to end-users and parents/guardians. Some examples would include:</p> <ul style="list-style-type: none"> <li>Periodic distribution of a newsletter reminding end-users and parents/guardians of their responsibilities when using the G-suite system.</li> <li>Refresher sessions can be conducted for end-users (students) at the start of each school term on the acceptable use policy for the system.</li> <li>Educational materials outlining the responsibilities of students and their parents/guardians distributed on a regular basis and in different formats to cater for a variety of knowledge levels.</li> </ul>

The following table shows the Directorate's risk ratings. Please refer to [Appendix D](#) for the full risk matrix.

Risk Rating	Response guidance
● Extreme	Risk must be reported to Senior Management and requires corrective measures or detailed treatment action plan/s to be implemented <i>immediately</i> to reduce the risk to Low or Medium.
● High	Risk must be reported to Senior Management and requires corrective measures or detailed treatment action plan/s to be implemented <i>as soon as practicable</i> to reduce the risk to Low or Medium.
● Medium	Specify management responsibility for treatment and/or monitoring.
● Low	Manage by routine procedures.

## 4. Detailed findings and recommendations

### 4.1 Governance accountabilities and responsibilities

#### Finding (High risk)

SSICT has been engaged to implement and manage the G-suite system for the Directorate. Since its deployment the G-suite system, along with associated management requirements, have gone through several changes. Although updates have been made to management activities for the system, the roles and responsibilities have not been clearly defined.

The G-suite project documentation does not clearly outline the roles and responsibilities of the teams within the Directorate and SSICT for managing the G-suite post implementation. Although there is a dedicated SSICT team assigned to provide daily support for end-users, the involvement of other teams within the Directorate and SSICT has not been formalised, and these additional teams are engaged on an as-needed basis.

There is no formal service level agreement in place between the Directorate and SSICT which outlines the roles and responsibilities of the support teams for the different components and management elements of the system. Service level agreements are key enablers in providing assurance that management expectations are clearly communicated to service providers and that services are provided to an acceptable level.

The review identified reporting to the Directorate associated with major incidents and security concerns raised during the Cyber Security risk forum, but did not identify other periodic/regular reporting to the Directorate (e.g. in relation to operational details of SSICT's management of the G-suite system). The G-suite support team indicated the Directorate requests operational data from time to time, but there is no regular reporting process currently established. Regular reporting of operational details supports effective governance of outsourced system support activities by enabling the Directorate to confirm that service performance and governance requirements are met.

#### Consequence

The lack of sufficient clarity on roles and responsibilities increases the risk of gaps emerging with respect to governance controls over the G-suite system. These governance gaps can result in:

- Increased probability and incidents of misuse, exploitation of control weaknesses, and security incidents; and
- Inability of the Directorate and SSICT to promptly identify and remediate such incidents to minimise any impact to the system, organisation, and end-users.

#### Recommendation 1

The Directorate should continue to engage with SSICT to clarify and document roles and responsibilities associated with management of the G-suite system. Regular compliance reviews should also be performed to:

- a. maintain adherence to agreed roles and responsibilities;
- b. provide an opportunity to re-educate the Directorate and SSICT teams on their roles and responsibilities; and
- c. provide an opportunity to re-assess and improve team accountabilities based on the current use, structure, and management capabilities of the G-Suite system.

**Management response: Agree, ACT Education has engaged with Digital Data and Technology Solutions (DDTS, previously known as SSICT) to agree and document roles, responsibilities and service expectations.**

**Responsible officer:** Ross Hawkins, Executive Group Manager, Service Design and Delivery, ACT Education. Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education

**Timeframes: Agreement documented by 30 June 2021**



## 4.2 Guidance and security standards

### Finding (Medium risk)

SSICT Standards are used as guidance for the proper configuration and management of the G-suite system. The more stringent security standards from either SSICT or the Directorate cannot be fully applied due to the ease-of-use requirements for the system's end-users (students). Without specific guidance on acceptable standards for the system, there is an inability to verify that relevant controls have been established for the configuration and management of the system.

Based on stakeholder consultations, certain operational principles have been established between the Directorate and SSICT, however these are yet to be formalised and reviewed to ensure that all the risk areas have been addressed.

### Consequences

Without the necessary guidance and security standards, the current governance process cannot assure that appropriate mitigating controls are considered and put in place to manage any standards deviation in either the configuration or management of the system. This could lead to similar incidents of inappropriate use of system features.

### Recommendation 2

The Directorate should:

- a. establish specific governance and security control standards appropriate to SSICT, the Directorate and end-users of the G-suite system. There is a G-suite security checklist that can be used as a base to establish the necessary built-in configuration items. These items will need to be customised to align with the Directorate's acceptable risk appetite.
- b. work closely with the vendor to provide regular training and support for the teams managing the system to progressively improve in-house capabilities.

For example, instead of requiring complex passwords that students may not be able to recollect, passphrases can be used instead. A thirteen (13) character non-case sensitive with all alphabetic passphrase takes seven times longer to crack than the traditional eight (8) character comprised of alphanumeric characters and symbols.

### Management response:

- a) **Partially Agreed**
  - **ACT Education has established routine checks, including a Directorate validation in each Term break. DDTS are responsible to implementing any changes into production, and therefore all security and settings are reviewed by the Technology and Security teams. The Security and Risk Management Plan is updated every three years. External security experts are sourced to review the environment every two years, this will continue, with the ongoing regular advice from DDTS.**
  - **Complex passwords is not appropriate for young students, these settings and risks will be reviewed every two years.**
- b) **Agreed, ACT Education has arranged System Admin review and training for DDTS, and any other relevant staff to build inhouse (ACTPS) capabilities.**

**Responsible officer:** Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education

**Timeframes:** 30 June 2021

### 4.3 System design documentation

#### Finding (Medium risk)

The following deficiencies were identified with respect to design documentation for the G-suite system:

- The documentation has not been updated since 2014 and does not reflect the current state of the system.
- The documentation does not include, or refer to, any integration mapping details for related systems. Details on broader system integration and networks is required to effectively perform assessments and reviews of the environment by providing a holistic view of the system together with interdependencies.
- Security considerations and mitigating controls for application features are not specifically highlighted to address the application's specific use-case (i.e. end-users are minors). Security standards for systems are required to be customised for their specific use-case to be effective.
- Roles and responsibilities for managing the system post implementation between the Directorate and SSICT teams are not defined. This creates gaps in the governance and oversight of the system.

Based on interviews and process reviews, information on the current state of the system is spread across a number of systems between the Directorate and SSICT. Currently, it requires significant effort to collect the necessary updated information on the configuration of the G-suite system within the IT environment. This impacts the effectiveness of change and incident management processes.

#### Consequences

Insufficient documentation of design details degrades the effectiveness of the design review process and subsequently the assurance it provides that key control considerations have been taken into account as part of the change management process.

#### Recommendation 3

The Directorate should:

- a. update the current design documentation to address the weaknesses observed.
- b. consider integrating a design documentation update process with change and incident management processes to ensure records are kept up to date and consequently improve the overall effectiveness of IT operations.
- c. Review and update the Change Management process, of all systems to consider the impact of other integrated or connected systems.

#### Management response:

- a) **Agreed, ACT Education will commission DDTS to update the design documents, including interfaces**
- b) **Partially Agreed,**
  - **ACT Education will commission DDTS to review the Change Management process, ensuring that the Technical Review point includes Technical Impact Assessment**
  - **ACT Education will engage DDTS to review the initial response approach for Major Incidents, to reduce the response time minimising the exposure. Technical documentation will be used throughout the Major Incident process, however**

**adding documentation review effort into the triage time would increase an issue similar to this issue. Initial response and containment is a critical first step, to then allow the technicians to triage and diagnose.**

- c) Agreed, ACT Education has extended to the ACTPS Change Management process to provide assurance relating Technical Impact Assessment , and Business Impact Assessment. ACT Education will commission DDTS to update the Technical Review process to include Technical Impact Assessment.**

**Responsible officer:** Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education

**Timeframes:** 30 September 2021

## 4.4 Monitoring over G-suite configuration and usage

### Finding (Medium risk)

The engagement included a review of the management activities that SSICT performs on the G-suite system. Management of the G-suite system is performed by the SSICT Edu team which includes monitoring of the application. Stakeholder consultations with the SSICT Edu team indicated current monitoring procedures involve reviews of built-in security features and settings within the application. The monitoring procedures do not include monitoring of anomalous usage due to limitations on data that can be accessed and traditional automated security tools cannot be utilised.

The post incident analysis performed by Foresight Consulting (refer [Appendix B](#)) was also reviewed and this highlighted similar observations. As part of the post-incident activities, the relevant alerts and notification settings have been reviewed and enabled to improve current monitoring capabilities.

### Consequences

Limited monitoring capabilities impair the ability to promptly detect and respond to any incidents.

### Recommendation 4

The Directorate should continue to engage with SSICT to ensure regular reporting of monitoring results and exceptions is performed by SSICT and submitted to the Directorate for review. The Directorate should review any exceptions reported in terms of compliance with approved policies and procedures. Exceptions should also be assessed as to whether they represent possible weaknesses in current system and management controls for the G-Suite system.

In the interim (while more robust monitoring processes are being developed), SSICT and the Directorate should maximise the use of existing features within the application to support improved monitoring of the application. For example:

- Data from G-Suite Highlights report could be used to perform further analysis to identify indicators of anomalous usage of features within the application; and
- Dummy accounts could be set up to detect similar incidents and monitor what is publicly distributed within the application.
- The Directorate should continue to engage with SSICT Major Incident process to ensure triaging process, including notification and expert advice be sought from the Directorate

### Management response:

#### Partially Agreed

- a) **ACT Education will commission DDTS to produce Managed Service Operational reports. ACT Education has setup Google alerts, these alerts are reviewed during each Term break.**
- b) **Dummy accounts are already available in the Google environment for testing purposes.**
- c) **Agreed, ACT Education will continue to engage with DDTS for Major Incident response.**

**Responsible officer:** Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education

**Timeframes:** 31 December 2021

## 4.5 Ongoing communication to students and parents/guardians

### Finding (Medium risk)

Based on the review of operational processes for managing the Directorate's G-suite system, there is no evidence of programs focused on managing and educating users.

As part of standard practice for managing IT systems, guidance should be established for end-users to ensure the system is used in accordance with the established acceptable use policy. This would typically be accomplished through publication of the current acceptable use policy which would allow users easy access to the information; performing periodic refresher courses; and providing regular communications on policy updates and reminders.

As demonstrated by the incident, increased rigour is required to ensure that proper end-user behaviour is reinforced to avoid cases of misuse of the G-suite system and associated resources.

As end-users are primarily comprised of minors, parents/guardians need to be engaged to help support initiatives aimed at promoting acceptable behaviour when using the G-suite system.

### Consequence

As primary users of the G-suite are minors, there is an increased risk of misuse and exploitation without adequate supervision/guidance from parents and guardians.

### Recommendation 5

Guidance on acceptable use of the system should be regularly communicated to end-users and parents/guardians. Some examples would include:

- Periodic distribution of a newsletter reminding end-users and parents/guardians of their responsibilities when using the G-suite system;
- Refresher sessions can be conducted for end-users (students) at the start of each school term on the acceptable use policy for the system;
- Educational materials outlining the responsibilities of students and their parents/guardians distributed on a regular basis and in different formats to cater for a variety of knowledge levels.

### Management response:

#### Completed

- **ACT Education completes the current ICT acceptable and eSafety programs:**
  - **Annually Parents, Carers and Students sign the acceptable ICT use agreement**
  - **Each Term a reminder and eSafety lesson is conducted**
  - **Throughout the year ACT Education partners with AFP to run ThinkUKnow programs for Parents and Carers**
  - **Throughout the year ACT Education engages with the eSafety Commissioner to participate in their:**
    - **Teacher sessions**
    - **Student sessions**
    - **Parents and Carer sessions**

**Responsible officer:** : Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education

**Timeframes:** Complete

## 5. Recommendations and management response

No.	Recommendations	Management Comment	Responsible Officer	Timing	Rating
1	<p>The Directorate should continue to engage with SSICT to clarify and document roles and responsibilities associated with management of the G-suite system. Regular compliance reviews should also be performed to:</p> <ul style="list-style-type: none"> <li>a. maintain adherence to agreed roles and responsibilities;</li> <li>b. provide an opportunity to re-educate the Directorate and SSICT teams on their roles and responsibilities; and</li> <li>c. provide an opportunity to re-assess and improve team accountabilities based on the current use, structure, and management capabilities of the G-Suite system.</li> </ul>	<p><b>Agree, ACT Education has engaged with Digital Data and Technology Solutions (DDTS, previously known as SSICT) to agree and document roles, responsibilities and service expectations.</b></p>	<p>Ross Hawkins, Executive Group Manager, Service Design and Delivery, ACT Education. Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education</p>	<p><b>30 June 2021</b></p>	<p>High</p>
2	<p>The Directorate should:</p> <ul style="list-style-type: none"> <li>a. establish specific governance and security control standards appropriate to SSICT, the Directorate and end-users of the G-suite system. There is a G-suite security checklist that can be used as a base to establish the necessary built-in configuration items. These items will need to be customised to align with the Directorate's acceptable risk appetite.</li> <li>b. work closely with the vendor to provide regular training and support for the teams</li> </ul>	<p><b>a) Partially Agreed</b></p> <ul style="list-style-type: none"> <li>• <b>ACT Education has established routine checks, including a Directorate validation in each Term break. DDTS are responsible to implementing any changes into production, and therefore all security and settings are reviewed by the Technology and Security teams. The Security and Risk Management Plan is updated every three years. External security experts are sourced to review the environment every two years, this</b></li> </ul>	<p>Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education</p>	<p><b>30 June 2021</b></p>	<p>Medium</p>



No.	Recommendations	Management Comment	Responsible Officer	Timing	Rating
	managing the system to progressively improve in-house capabilities.	<p>will continue, with the ongoing regular advice from DDTS.</p> <ul style="list-style-type: none"> <li>• Complex passwords is not appropriate for young students, these settings and risks will be reviewed every two years.</li> </ul> <p>b) Agreed, ACT Education has arranged System Admin review and training for DDTS, and any other relevant staff to build inhouse (ACTPS) capabilities.</p>			
3	<p>The Directorate should:</p> <ol style="list-style-type: none"> <li>a. update the current design documentation to address the weaknesses observed.</li> <li>b. consider integrating a design documentation update process with change and incident management processes to ensure records are kept up to date and consequently improve the overall effectiveness of IT operations.</li> <li>c. Review and update the Change Management process, of all systems to consider the impact of other integrated or connected systems.</li> </ol>	<ol style="list-style-type: none"> <li>a) Agreed, ACT Education will commission DDTS to update the design documents, including interfaces</li> <li>b) Partially Agreed, <ul style="list-style-type: none"> <li>• ACT Education will commission DDTS to review the Change Management process, ensuring that the Technical Review point includes Technical Impact Assessment</li> <li>• ACT Education will engage DDTS to review the initial response approach for Major Incidents, to reduce the response time minimising the exposure. Technical documentation will be used throughout the Major Incident process, however adding documentation review effort into the triage time would increase an issue similar to this issue. Initial response and containment is a critical first step, to then allow the technicians to triage and diagnose.</li> </ul> </li> </ol>	Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education	30 September 2021	Medium

No.	Recommendations	Management Comment	Responsible Officer	Timing	Rating
		<p>c) Agreed, ACT Education has extended to the ACTPS Change Management process to provide assurance relating Technical Impact Assessment, and Business Impact Assessment. ACT Education will commission DDTS to update the Technical Review process to include Technical Impact Assessment.</p>			
4	<p>The Directorate should continue to engage with SSICT to ensure regular reporting of monitoring results and exceptions is performed by SSICT and submitted to the Directorate for review. The Directorate should review any exceptions reported in terms of compliance with approved policies and procedures. Exceptions should also be assessed as to whether they represent possible weaknesses in current system and management controls for the G-Suite system.</p> <p>In the interim (while more robust monitoring processes are being developed), SSICT and the Directorate should maximise the use of existing features within the application to support improved monitoring of the application. For example:</p> <ul style="list-style-type: none"> <li>• Data from G-Suite Highlights report could be used to perform further analysis to identify indicators of anomalous usage of features within the application; and</li> <li>• Dummy accounts could be set up to</li> </ul>	<p><b>Partially Agreed</b></p> <p>a) ACT Education will commission DDTS to produce Managed Service Operational reports. ACT Education has setup Google alerts, these alerts are reviewed during each Term break.</p> <p>b) Dummy accounts are already available in the Google environment for testing purposes.</p> <p>c) Agreed, ACT Education will continue to engage with DDTS for Major Incident response.</p>	Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education	31 December 2021	Medium



No.	Recommendations	Management Comment	Responsible Officer	Timing	Rating
	detect similar incidents and monitor what is publicly distributed within the application.				
5	<p>Guidance on acceptable use of the system should be regularly communicated to end-users and parents/guardians. Some examples would include:</p> <ul style="list-style-type: none"> <li>• Periodic distribution of a newsletter reminding end-users and parents/guardians of their responsibilities when using the G-suite system;</li> <li>• Refresher sessions can be conducted for end-users (students) at the start of each school term on the acceptable use policy for the system;</li> <li>• Educational materials outlining the responsibilities of students and their parents / guardians distributed on a regular basis and in different formats to cater for a variety of knowledge levels.</li> </ul>	<p><b>Completed</b></p> <ul style="list-style-type: none"> <li>• <b>ACT Education completes the current ICT acceptable and eSafety programs:</b> <ul style="list-style-type: none"> <li>○ <b>Annually Parents, Carers and Students sign the acceptable ICT use agreement</b></li> <li>○ <b>Each Term a reminder and eSafety lesson is conducted</b></li> <li>○ <b>Throughout the year ACT Education partners with AFP to run ThinkUKnow programs for Parents and Carers</b></li> <li>○ <b>Throughout the year ACT Education engages with the eSafety Commissioner to participate in their:</b> <ul style="list-style-type: none"> <li>▪ <b>Teacher sessions</b></li> <li>▪ <b>Student sessions</b></li> <li>▪ <b>Parents and Carer sessions</b></li> </ul> </li> </ul> </li> </ul>	Kelly Bartlett, Executive Branch Manager, Chief Information Officer, ACT Education	<b>Completed</b>	Low

## Appendix A – Key Control Considerations for Managing/Configuring G-Suite

The below list describes control practices that the Directorate should consider adopting to improve overall management of the G-suite system:

### Governance

- Change management processes that acknowledge constant changes/configurations for google suite and report accordingly
- Advisory mechanism for Business System owners for known threats/vulnerabilities/changes and recommended/required security configurations
- Review business function and assign risk owners with capability to respond to events/incidents

### Documentation

- Business Impact Levels for all business systems
- Data Management Plan
- SRMP's, SRS's and System security plans for all business systems
- Working group/advisory model for known bugs/issues
- Incident Response Plans
- Patch management plans

### Practices

- Risk and Governance advisory group

## Appendix B – Foresight Consulting Review

The Directorate engaged Foresight Consulting during the incident to provide real-time advice and assurance with respect to the Directorate's incident response. In summary, the services provided by Foresight Consulting included:

- **Part 1:** Readiness Assurance – Google Services (excluding Gmail) – Confirm the actions taken by the Directorate since the incident were appropriate, and the Google services platform (excluding Gmail) could be un-blocked.
- **Part 2:** Readiness Assurance – Gmail Services - Confirm the actions taken by the Directorate since the incident were appropriate, and the Gmail services could be un-blocked.
- **Part 3:** A more comprehensive Post Incident Review of what took place, and consideration for any related vulnerabilities that may exist in the Directorate's response.

Findings from the Foresight Consulting Review were shared with, and considered by, PwC in conducting its post incident review.

## Appendix C – RACI recommendation

The below definitions are used in the below chart, when discussing responsible, accountable, consulted and informed.

- **Responsible** - refers to the team, individuals, or business unit who is required to perform the activities and management practices for Directorate systems managed by SSICT.
- **Accountable** - refers to the team, individuals, or business unit who delegates activities and management practices for Directorate systems managed by SSICT.
- **Consulted** - refers to the team, individuals, or business unit who may be required to perform input into activities and management practices for Directorate systems managed by SSICT. The input may be taken into account by those accountable and responsible for performing the activities and management practices
- **Informed** - teams, individuals, or business units who may be provided updates based on the outcome of activities and management practices for Directorate systems managed by SSICT.

Activity	The Directorate		Shared Services ICT	
	Executive Management	IT Department	Edu Support Team	Infrastructure & Security team
<b>Governance Policies and Standards</b> - Establish, operate, and maintain customised policies and standards to identify, analyse, and mitigate risk to the system, including related interconnected infrastructure	I	R, A	R	C
<b>System Documentation</b> - Manage system documentation to assure that it is updated and periodically reviewed for accuracy with current system configuration	I	A, C	R	R
<b>Change and configuration management</b> - Manage the organization's information technology (IT) and operations technology (OT) assets commensurate with the risk to critical infrastructure and organizational objectives.	I	C	A, R	C
<b>Security Management</b> - Establish and maintain plans, procedures, and technologies to detect, identify, analyse, manage, and respond to threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives	I	C	R	A
<b>Monitoring and Control</b> - Establish and maintain activities and technologies to collect, analyse, alarm, present, and use system information to form a common operating picture	I	A	R	C

## Appendix D – Directorate risk matrix



Last Update: 04 Sept 2018

		Consequence **				
		Insignificant	Minor	Moderate	Major	Catastrophic
<b>Financial</b>		1% of Budget or <-\$5K	2.5% of Budget or <-\$50K	> 5% of Budget or <-\$500K	> 10% of Budget or <-\$5M	>25% of Budget or >-\$5M
<b>People</b>		Injury or ailments not requiring First Aid treatment and / or psychological injury managed by staff support services.	Minor injury or requiring First Aid treatment or short term injury (less than four weeks incapacity for work) and / or psychological injury resulting in reduced ability to perform tasks requiring treatment from a health professional.	Serious injury causing hospitalisation or medium term reversible disability (four weeks or more incapacity for work) or multiple medical treatment cases and / or psychological injury resulting in reduced ability to perform tasks requiring ongoing support from GP/health professional.	Single life threatening injury (including loss of limbs) or multiple serious injuries causing hospitalisation and/or permanent disability and / or psychological injury resulting in reduced ability to perform tasks requiring significant additional psychological treatment.	Death or multiple life threatening injuries and/or multiple injuries causing major life altering impairment and / or psychological injury resulting in inability to perform tasks requiring ongoing significant psychological treatment.
<b>Compliance/ Regulation</b>		Non-compliance with work policy and standard operating procedures which are not legislated or regulated.	Numerous instances of non-compliance with work policy and standard operating procedures which are not legislated or regulated.	Non-compliance with work policy and standard operating procedures which require self reporting to the appropriate regulator and immediate rectification.	Restriction of business operations by regulator due to non-compliance with relevant guidelines and / or significant non-compliance with policy and procedures which threaten business delivery.	Operations shut down by regulator for failing to comply with relevant guidelines / legislation and /or significant non-compliance with internal procedures which could result in failure to provide business outcomes and service delivery.
<b>Reputation &amp; Image</b>		Internal review and/or minor dissatisfaction across a small number of demographic groups or stakeholders.	Scrutiny required by internal committees or internal audit to prevent escalation and/or moderate dissatisfaction across a small number demographic groups or several stakeholders.	Local media scrutiny (1 week) and/or scrutiny required by external committees or ACT Auditor General's Office, or Inquest, etc. and/or dissatisfaction across a few demographic groups or multiple stakeholders.	Intense public, political and national media scrutiny (1 week) and/or Minister / Chief minister involvement and/or dissatisfaction across a large range of demographic groups and stakeholders.	Adverse finding from Assembly Inquiry or Commission of Inquiry or sustained adverse international media and/or loss of public confidence in Govt or Public Service forcing changes to the machinery of Govt.
<b>Service Delivery</b>		Loss of or interruption to non critical/no-core services up to 3 days.	Interruption of core services affecting critical infrastructure (e.g. law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days.	Cessation of core services affecting critical infrastructure (e.g. law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days and/or disruption for a week.	Cessation of core services affecting critical infrastructure (e.g. law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days and/or disruption over subsequent weeks.	Total cessation of core services affecting critical infrastructure (e.g. law & order, public safety, health) or cessation of core/ critical service essential to business continuity for more than 1 week and/or disruption over subsequent months.

Likelihood of Consequence	Frequency		Matrix					
			1	2	3	4	5	
	<b>Almost Certain</b>	Is expected to occur in most circumstances	Once in a quarter or more	5	High	High	Extreme	Extreme
	<b>Likely</b>	Will probably occur	Once a year or more	4	Medium	High	High	Extreme
	<b>Possible</b>	Might occur at some time in the future	Once every 1 - 5 years	3	Low	Medium	High	Extreme
	<b>Unlikely</b>	Could occur but doubtful	Once every 5 - 20 years	2	Low	Medium	High	High *
<b>Rare</b>	May occur but only in exceptional circumstances	Once every 20 - 100 years	1	Low	Low	Medium	High *	

Priority for Attention / Action *				
Priority	Indicative Escalation	Indicative Action Plan	Authority for Action	Optional Considerations
<b>Extreme</b>	Within 24 hours	1 month or sooner	DG & DDG (CEO or equivalent)	Chair ARMC Director WH&S
<b>High</b>	Within 7-14 days	2 months or sooner	Senior Executive or equivalent (DDG/ED/Head of Agency or equivalent)	Director WH&S
<b>Medium</b>	Within 1-3 months	3 months or sooner	Executive/Business Unit Head/Manager	WH&S Team
<b>Low</b>	1-3 months in course of normal business	3-6 months or sooner	Team Leader/Supervisor	WH&S Team

Risk Control Effectiveness	
Control Effectiveness	Guide
<b>Adequate</b>	Controls are well designed and operating effectively in treating the root cause of the risk. Additional controls exist to appropriately manage consequence. Nothing further to be done except review and monitor the existing controls. Controls are largely preventative and management believes that they are effective and reliable at all times.
<b>Room for Improvement</b>	Some deficiencies in controls have been identified however most controls are designed and implemented effectively in treating the root cause of the risk. While some preventative controls exist, controls are largely reactive. There are opportunities to improve the design/implementation of some controls to improve operational effectiveness.
<b>Inadequate</b>	Some deficiencies in controls have been identified however most controls are designed and implemented effectively in treating the root cause of the risk. While some preventative controls exist, controls are largely reactive. There are opportunities to improve the design/implementation of some controls to improve operational effectiveness.



Category of Risk	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Assets	Loss or destruction of assets up to \$2,000.	Loss or destruction of assets \$2,000 to \$10,000.	Loss or destruction of assets \$10,000 to \$100,000.	Loss or destruction of assets \$100,000 to \$5M.	Loss or destruction of assets greater than \$5M.
Compliance/ Regulation	Non-compliance with work policy and standard operating procedures which are not legislated or regulated.	Numerous instances of non-compliance with work policy and standard operating procedures which are not legislated or regulated.	Non-compliance with work policy and standard operating procedures which require self reporting to the appropriate regulator and immediate rectification.	Restriction of business operations by regulator due to non-compliance with relevant guidelines and / or significant non-compliance with policy and procedures which threaten business delivery.	Operations shut down by regulator for failing to comply with relevant guidelines / legislation and / or significant non-compliance with internal procedures which could result in failure to provide business outcomes and service delivery.
People	Injury or ailments not requiring First Aid treatment and/or psychological injury managed by staff support services.	Minor injury or requiring First Aid treatment or short term injury (less than four weeks incapacity for work) and/or psychological injury resulting in reduced ability to perform tasks requiring treatment from a health professional.	Serious injury causing hospitalisation or medium term reversible disability (four weeks or more incapacity for work) or multiple medical treatment cases and/or psychological injury resulting in reduced ability to perform tasks requiring ongoing support from GP/health professional.	Single life threatening injury (including loss of limbs) or multiple serious injuries causing hospitalisation and/or permanent disability and/or psychological injury resulting in reduced ability to perform tasks requiring significant additional psychological treatment.	Death or multiple life threatening injuries and/or multiple serious injuries causing major life altering impairment and/or psychological injury resulting in inability to perform tasks requiring ongoing significant psychological treatment.
Environment	Limited effect to something of low significance and/or effects are limited to a small area with rapid recovery.	Transient, minor effects and/or minor effects to environment and/or disturbance of native vegetation or waterways.	Moderate, short-term environmental harm to environment and/or disturbance of native vegetation or waterways.	Significant, medium-term environmental harm to environment and/or disturbance of native vegetation or waterways.	Long term environmental harm and/or widespread or severe impacts to environment, threatened species and/or long term effects on ecological community or native vegetation or waterways.
Financial	1% of Budget or <\$5K	2.5% of Budget or <\$50K	> 5% of Budget or <\$500K	> 10% of Budget or <\$5M	>25% of Budget or >\$5M
Service Delivery	Loss of or interruption to non critical/no-core services up to 3 days.	Interruption of core services affecting critical infrastructure (eg law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days.	Cessation of core services affecting critical infrastructure (eg law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days and/or disruption for a week.	Cessation of core services affecting critical infrastructure (eg law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days and/or disruption over subsequent weeks.	Total cessation of core services affecting critical infrastructure (eg law & order, public safety, health) or cessation of core/ critical service essential to business continuity for more than 1 week and/or disruption over subsequent months.
Information & Records Management	Interruption to ICT systems, electronic records and data access less than ½ day and/or system breach to business administration system with no personal or classified information stored.	Interruption to ICT systems, electronic records and data access 1/2 - 1 day and/or system breach to business administration system with some identifiable information but non-client threatening (data access known).	Significant interruption (but not permanent loss) systems and data access 1-7 days and/or system breach to business administration system with some identifiable information but non-client threatening (data access unknown).	Complete, permanent loss of some electronic records and/or data, or loss of access to ICT systems and data for more than 7 days and/or systems breach to business administration system with identifiable/classified information stored but non-client welfare threatening.	Complete, permanent loss of or inability to recover/reconstruct all records and data and/or total loss of confidence in data/record integrity and/or systems breach to Govt or business critical systems with client and/or business welfare threatened.
Reputation & Image	Internal review and/or minor dissatisfaction across a small number of demographic groups or stakeholders.	Scrutiny required by internal committees or internal audit to prevent escalation and/or moderate dissatisfaction across a small number demographic groups or several stakeholders.	Local media scrutiny (1 week) and/or scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc and/or dissatisfaction across a few demographic groups or multiple stakeholders.	Intense public, political and national media scrutiny (1 week) and/or Minister / Chief minister involvement and/or dissatisfaction across a large range of demographic groups and stakeholders.	Adverse finding from Assembly inquiry or Commission of inquiry or sustained adverse international media and/or loss of public confidence in Govt or Public Service forcing changes to the machinery of Govt.
Cultural & Heritage	Low-level repairable damage to commonplace structures.	Mostly repairable damage to items of cultural and/or heritage significance.	Significant damage to items of cultural and/or heritage significance.	Permanent damage to structures or items of cultural and/or heritage significance.	Irreparable damage to or loss of highly valued items of cultural and/or heritage significance.
General Business Activities	Minor errors in systems or processes requiring corrective action and/or minor delay without impact on overall schedule and/or insignificant impact on business outcomes and strategic objectives and/or negligible disruption to services or non-essential subsidiary services.	Policy procedural rule occasionally not met and/or services do not fully meet need and/or minor impact on business outcomes and strategic objectives and/or non-essential or subsidiary services experience minor disruptions.	One or more key accountability requirements not met and /or inconvenient but not client welfare threatening and/or moderate impact on business outcomes and strategic objectives and/or a number of objectives not met, minor or subsidiary services	Significant impact on business and / or strategic objectives and/or strategies not consistent with Government's agenda and/or trends show service is degraded and/or key service delivery impaired.	Strategic business outcomes processes fail, control infrastructure failure, critical business objectives not met. Unable to deliver necessary critical services.

## Appendix E – Stakeholder consultations

Key stakeholders consulted with during the review included:

Position
Executive Group Manager, Service Design and Delivery, Education Directorate
A/g Executive Branch Manager, Digital Strategy, Services & Transformation / Chief Information Officer, Education Directorate
a/g Service Manager, Digital, Data and Technology Solutions, Chief Minister, Treasury and Economic Development Directorate
Assistant Director, Customer Engagement Services Branch, Digital, Data and Technology Solutions, Chief Minister, Treasury and Economic Development Directorate
ICT Change Manager, Digital, Data and Technology Solutions, Chief Minister, Treasury and Economic Development Directorate
AD/FIM, Digital, Data and Technology Solutions, Chief Minister, Treasury and Economic Development Directorate

## Appendix F – Key Documentation Reviewed

Document	Provided by
Conceptual Solution Design - Project: Digital Schools Platform - Project code: 67638 - Chief Minister, Treasury and Economic Development Directorate, Shared Services ICT	Education Directorate
Privacy Impact Assessment - Microsoft Office 365 and Google Apps for Education – Information Integrity Solutions	Education Directorate
Assessment of ETD Information against the PSPF, Enabling Measured Transition to Cloud Services – Red Core	Education Directorate
Teach Anywhere Security and Risk Management Plan	Education Directorate
Education Cyber Security Committee Papers	Education Directorate
SSICT Security Standards and Policies	SSICT Security team