10.1.1 Manual logs

The manual logs if any that relate to this system are:	N/A

Audit Log Protection

Who has access to the audit log?	DDTS Administrators
Where are the results of the audit log analysis stored? (This is important if it contains personal information)	Within the system.

Audit Log Retention

Is the audit log retained on-line indefinitely, or is its contents periodically archived?	Audit logs are kept online for 6 months before being deleted. (See summary table below)
The method for archiving the audit log is:	N/A
6 months	6 months See https://support.google.com/a/answer/7061566?hl=en (see summary table below)

10.1.2 Available audit logs

In the Google Admin console, we can review user and administrator activity of the organization. Can use the information to track users and admins and for security purposes.

Google Workspace provides audit logs at the Google Cloud organization level as follows:

- Google Workspace Enterprise Groups Audit Writes Admin Activity audit logs only.
- Google Workspace Admin Audit Writes Admin Activity audit logs only.
- Google Workspace Login Audit Writes Data Access audit logs only.

For more information, please refer to https://cloud.google.com/logging/docs/audit/gsuite-audit-logging

Admin activities

Audit log	Description
Admin audit log	View admin activity in the Google Admin console
Groups Enterprise audit log	See Admin console actions on groups and group memberships

Security

Audit log	Description
Access Transparency logs	See Google staff actions' when accessing your data
Login audit log	Track user sign-in activity
OAuth Token audit log	Track third-party app usage and data-access requests
Rules audit log	Track your users' attempts to share sensitive data
SAML audit log	View your users' sign-ins to SAML applications
Secure LDAP audit log	Review LDAP operations for the Secure LDAP service

User services and accounts

Audit log	Description
Calendar audit log	View and track changes to user events in Google Calendar
Chrome audit log	View Chrome events for your organization
Context-Aware Access audit log	Use data to troubleshoot users' access to apps
Currents audit log	Track Currents activity for your organization
Data Studio audit log	View users' actions in Google Data Studio
Devices audit log	Review activities on your organization's devices

Audit log	Description
Drive audit log	View user Google Drive activity
Email Log Search	Track the delivery of email messages
Google Chat audit log	Track user conversations and room activity
Google Meet audit log	Understand users' video-meeting activity
Graduation audit log	Track user data transfer
Groups audit log	View user changes to groups in Google Groups
Jamboard audit log	Track changes to Jamboards
Password Vault audit log	See admin and user activity related to password vaulted apps
Takeout audit log	View user Google Takeout activity
User accounts audit log	View user activity across their accounts
Voice audit log	Review user activity in Google Voice

10.1.3 Audit Data retention and lag times

The admin console reports, and audit logs don't show the latest data, because reports don't reflect real-time data. The lag times in the table below show how long it can take before data for specific Admin console reports and audit logs is available. Some reports might take longer to display updated information.
Important: There's a small chance that reports and audit logs for some events will be delayed beyond the specified times below. In very rare cases, events may not be reported.

Lag times

The lag times in this table show how long it can take before data for specific Admin console reports and audit logs is available.

Highlights

Item name	Report name	Lag time
Calendar	Calendar report	1–3 days
Classroom	Classroom report	1–3 days
Currents	Currents report	1–3 days
Document link shared status	Drive report	1–3 days
Drive	Drive report	1–3 days
Gmail	Gmail report	1–3 days
Hangouts	Hangouts report	1–3 days

Security

Item name	Report name	Lag time
2-Step Verification Enrolment	2-Step Verification Enrolment report	1–3 days
External apps	External apps report	1–3 days
External shares	External shares report	1–3 days
Internal shares	Internal shares report	1–3 days

Aggregate reports

Item name	Report name	Lag time
Accounts	Accounts report	1–3 days
Apps Script	Apps Script report	1–3 days
Chrome	Apps and extension usage report	1–3 days
Chrome	Version report	1–3 days
Currents	Currents report	1–3 days
Drive	Drive report	1–3 days
Gmail	Gmail report	1–3 days
Google Chat	Google Chat report	1–3 days
Mobile	Mobile report	1–3 days

Apps usage activity

Item name	Report name	Lag time
Drive storage used	Drive storage used report	1–3 days
Files added	Files added report	1–3 days
Files edited	Files edit report	1–3 days
Files viewed	Files viewed report	1–3 days
Gmail storage used	Gmail storage used report	1–3 days
Google Sheets added	Google Sheets added report	1–3 days
Photos storage used	Photo storage used report	1–3 days
Total storage used	Total storage used report	1–3 days

Audit

Item name	Report name	Lag time
Access Transparency	Access Transparency audit	near real time (couple of minutes)
Admin	Admin audit	near real time (couple of minutes)
Calendar	Calendar audit	tens of minutes (can also go up to a couple of hours)
Chat	Chat audit	1–3 days
Currents	Currents audit	1–3 days
Data Studio	Data Studio audit	near real time (in most cases, a couple of minutes)
Drive	Drive audit	near real time (couple of minutes)
Email log search	Email audit	1–3 days
Groups	Groups audit	tens of minutes (can also go up to a couple of hours)
Jamboard	Jamboard audit	1–3 days
LDAP	LDAP audit	1–3 days
Login	Login audit	up to a few hours
Meet	Meet audit	near real time (couple of minutes)
Meet quality tool	Meet quality	near real time (couple of minutes)
Mobile devices	Devices audit	up to a few hours
SAML	SAML audit	up to a few hours
Token	Token audit	a couple of hours
User accounts	User accounts audit	tens of minutes
Voice	Voice audit	1–3 days

Retrieving report or audit log data for older dates or a wide time range might take so long that, by the time results are available, the most recent log data might no longer be fresh. For tools that require real-time monitoring, use a short time range.

How long is data saved?

You can access Admin console audit logs and reports data this far back:

Audit log or report name	Data retention time
Access Transparency	6 months
Account activity reports	6 months
Admin audit log	6 months
Audit data retrieved using the API	6 months
Calendar audit log	6 months
Chat audit log	6 months
Chrome apps and extension usage report	12 months (also configurable by admin)

Audit log or report name	Data retention time
Chrome version report	12 months (also configurable by admin)
Currents audit log	6 months
Customer/User usage data retrieved using the API	15 months
Data Studio audit log	6 months
Devices audit log (availability of these logs is dependent on your subscription)	6 months
Drive audit log (availability of these logs is dependent on your subscription)	6 months
Email log search	30 days
Entities usage data retrieved using the API	30 days
Groups audit log	6 months
Jamboard audit log	6 months
Login audit log	6 months
Meet audit log	6 months
Meet quality tool	30 days (Meetings older than 28 days are not displayed in the Admin Console)
OAuth Token audit log (availability of these logs is dependent on your subscription)	6 months
SAML audit log	6 months
Security reports	6 months
User accounts audit log	6 months
Voice audit log	6 months

Note: For reports and audit logs not mentioned here, the retention time is generally 6 months.
For more information, please refer to https://cloud.google.com/logging/docs/audit/services

10.2 Reporting and auditing

Audit and reporting are managed by the vendor on behalf of Education Directorate.

If an incident occurs, or a request from Education Directorate is received, the vendor provides the information. There is no interface for the admin or users to view and monitor audit logs outside of the Education Directorate Azure tenancy which is managed by ACT Government.

Google does produce Audit logs for all login and edit actions.

11 Incident Response

11.1 Security Points of Contact

Role	Name (if applicable)	Phone	Email
Vendor Account Manager	Customer Success Manager	(02)	
Administration Team	DDTS EDU ICT (Via DSST Service Desk)	02 620 76678	DSST@act.gov.au
ICT Security Operations on call	DDTS Security Operations	P - 6207 2038	DDTSSecurity@act.gov.au

11.2 Security Event Logging and Monitoring

An ICT security **event** is an identified occurrence of a system, service or network state indicating a possible breach of the Territory's ICT Security Policy or failure of controls, or a previously unknown situation that may be relevant to security.

☒	The Vendor logs security events relating to GSUITE-EDU-BS, including time and date.
☐	The Vendor monitors security logs 24x7 through a Security Operations Centre.
☐	The Vendor is notified by a third-party host of security incidents via email.
☐	The Vendor can view a summary of security announcements on a third-party host's website.
☐	EDU can review security logs on request.
☒	EDU is notified by the Vendor of security incidents via email.
☐	EDU can review a summary of security announcements on the Vendor website.
☐	The Vendor has agreed to provide DDTS with security logs to support incident response and investigate.
☒	The Vendor has agreed to provide access to security logs for ingestion into DDTS' Security Information and Event Management System (SIEM), and the SIEM has been configured to raise alerts of security events that are likely to be incidents.

11.3 Security Incident Response

An ICT security incident is a single or series of unwanted to unexpected ICT security events that have a significant probability of compromising business operations and threatening information security.

☒	The Vendor and EDU have exchanged contact details for their formal Security Points of Contact.
☒	EDU has obtained the Vendor's Security Incident Response Plan or equivalent.
☐	EDU has documented its Security Incident Response procedures as part of a Standard Operating Procedure or equivalent.
☒	Security Incident Response procedures include reporting all security incidents promptly to DDTS ICT Security.
☒	EDU system owner, system manager and system administrators have read and understood the ACT Government Security Incident Response Plan.

11.4 Data Breach Notification

A data breach is defined as unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information. A data breach that is eligible for mandatory notification arises when the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds
- this is likely to result in serious harm to one or more individuals (see Is Serious Harm Likely?), and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

☒	The Vendor is a regulated entity under the *Privacy Act (Cth)* and notifies the following parties of eligible data breaches: • EDU • Individuals to whom the information relates • Office of the Australian Information Commissioner
☒	EDU system owner has read and understood the *Notification of data breaches* policy of the ACT Government ICT Security Policy.

12 Physical, Environment and Media Protection

12.1 Hosting Arrangement

The System Owner and other stakeholders of the SSP must be aware of where their system is geographically hosted, and the physical security arrangements for the protection of hosted data.

☐	The application is hosted by DDTS, and its standard procedures for physical security have been verified as satisfactory.
☐	The application is hosted by DDTS in Microsoft Azure. The infrastructure that is part of Azure Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) is located strictly in AU datacentres with a minimum of SCEC 3 – beyond the accreditation suitable for hosting IMM or protected information. The physical security of systems like disk handling, disposal of infrastructure and other facets of physical security have reached accreditation at PROTECTED level as per the IRAP assessment of 2017 for Microsoft Azure cloud operations. For further discussion of security risks of the Azure platform, see the DDTS Azure Cloud SSP.
☐	The application is hosted by DDTS in Amazon Web Services (AWS). The infrastructure that is part of AWS Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) is located strictly in AU datacentres with a minimum of SCEC 3 – beyond the accreditation suitable for hosting IMM or protected information. AWS has achieved certification for physical security as part of the AWS IRAP assessment and is suitable for data up to an including OFFICIAL IMM. AWS is applying for PROTECTED certification which will include physical security, as part of the current IRAP assessment phase. For further discussion of security risks of the AWS platform, see the DDTS AWS Cloud SSP.
☒	Other (describe): Google is hosted Australia on Google infrastructure services. Google Cloud products are served from specific regional failure domains and are fully supported by Service Level Agreements to ensure you are designing your application architecture within the structure of Google Cloud. Google Cloud infrastructure services are available in locations across North America, South America, Europe, Asia, and Australia. These locations are divided into regions and zones. You can choose where to locate your applications to meet your latency, availability, and durability requirements. Regions are independent geographic areas that consist of zones. Zones and regions are logical abstractions of underlying physical resources provided in one or more physical data centres. These data centres may be owned by Google, and listed on the Google data centre location page, or they may be leased from third party data centre providers. Regardless of whether the data centre is owned or leased, Google Cloud selects data centres and designs its infrastructure to provide a uniform level of performance, security, and reliability. A zone is a deployment area for Google Cloud resources within a region. Zones should be considered a single failure domain within a region. To deploy fault-tolerant applications with high availability and help protect against unexpected failures, deploy your applications across multiple zones in a region. To protect against the loss of an entire region due to natural disaster, have a disaster recovery plan and know how to bring up your application in the unlikely event that your primary region is lost. Google Cloud's services and resources can be zonal, regional, or managed by Google across multiple regions.

https://cloud.google.com/about/locations#asia-pacific

Google Products available by location

Deploy resources in specific zones, regions and Mutli-regions

ASIA PACIFIC REGION

Products	Sydney (australia-southeast1)	Melbourne (australia-southeast2)
COMPUTE		
Compute Engine [5.6]	●	●
App Engine	●	
Google Kubernetes Engine [5.6]	●	●
Cloud Functions	●	
Cloud Run	●	●
Google Cloud Vmware Engine	●	
STORAGE & DATABASES		
Cloud Storage [2.5.6]	●	●
Cloud Storage for Firebase	●	
Cloud Bigtable [5]	●	●
Cloud Spanner [2.5.6]	●	●
Cloud SQL [5.6]	●	●
Firestore [4.5]	●	
Memorystore	●	●
Filestore [6]	●	●
Persistent Disk [5.6]	●	●
BIG DATA & MACHINE LEARNING		
BigQuery [2.5]	●	●
Cloud Composer	●	
Cloud Dataproc [5.6]	●	●
Cloud Data Catalog	●	●
Cloud Data Fusion	●	●
Cloud Datalab	●	●
Cloud Pub/Sub [1.6]	●	●
NETWORKING		
Virtual Private Cloud [1.6]	●	●
Cloud Load Balancing [1.6]	●	●
Cloud Interconnect	●	●
DEVELOPER TOOLS		
Artiface Registry	●	
Cloud Build	●	
Container Registry [2]		
Google Cloud Deploy		
IDENTITY & SECURITY		
Cloud Key Management Service [1.2.6]	●	●
Cloud Data Loss Prevention	●	
Cloud EKM	●	●
Cloud HSM	●	
Secret Manager	●	●
HEALTHCARE & LIFE SCIENCES		
Cloud Healthcare API	●	
API MANAGEMENT		
Apigee	●	
APPLICATION INTEGRATION		
API Gateway	●	
Cloud Scheduler	●	
Cloud Tasks	●	
Workflows		
MEDIA AND GAMING		
Trancoder API		

12.4 Network Communications infrastructure

☐	The application is hosted on-premises by DDTS, and all network communications takes place over the ACT Government's communications network: • The application uses only the ACT Government's network communications infrastructure, up to and including the DMZ, and DDTS's standard procedures apply[8]. • Beyond the DMZ, communications are over commercial carriers' infrastructure, and their physical security standards apply.
☐	The application is hosted by DDTS externally, in a third-party cloud platform or infrastructure (e.g. AWS and Azure). DDTS has documented the network communications from their data centre to the point its communications join the commercial carrier's infrastructure (e.g., shared fibre in a commercial data centre, or their own fibre in their own data centre)
☒	Other (describe): DDST manage the network and communications infrastructure needed to communicate and actively use the Google Workplace Services. Google's infrastructure includes network interfaces. Their data centres and network architecture are designed for maximum reliability and uptime. The workloads are securely distributed across multiple regions, availability zones, points of presence, and network cables to provide strong built-in redundancy and application availability.

12.5 Endpoint Infrastructure

The premises from which the application is accessed and the physical security arrangements at each type of site are (select all that apply):

☒	**ACT Government premises**: • access to the premises is controlled by swipe cards or keys • swipe cards are issued to verified staff and contractors only • all communications equipment on the site is in a Class C cabinet • separate recycling bins for sensitive and non-sensitive paper • laptop computers are the responsibility of individual staff
☒	**ACT Government Schools**: • Staff access is via internal keys and Cards • Student access is during school hours to an open school • Visitor access to the premises is controlled by physical sign-in at the front Office • all communications equipment on the site is in a Class C cabinet • separate recycling bins for sensitive and non-sensitive paper • desktop computers are secured in computer labs • laptop computers are the personal responsibility of teachers

[8] For details, contact DDTS Network Services

☒	**Vendor premises** The business processes for the application allow vendor remote access – where the Directorate cannot be sure of the physical security employed. (Describe): Enterprise network connectivity Enterprises connect existing on-premises infrastructure with their Google Cloud resources by evaluating the bandwidth, latency, and SLA requirements that help in choosing the best connection option: For low-latency, highly available, enterprise-grade connections that will enable to reliably transfer data between the on-premises and VPC networks without traversing the internet connections to Google Cloud, use Cloud Interconnect: - Dedicated Interconnect provides a direct physical connection between the on-premises network and Google's network. - Partner Interconnect provides connectivity between the on-premises and Google Cloud VPC networks through a supported service provider. For more details, please refer https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#networking_and_security The Google application is deployed on Google data centre infrastructure (see Figure 1) hosted in Australia. These data centres have physical access control restricted Google staff (https://www.google.com.au/about/datacenters/data-security/).
☒	**Other locations** The business processes for the application use requires infrastructure in other locations, such as users' homes where Directorate cannot be sure of the physical security employed. (Describe): Home: The business processes for the application allow remote access from home – where the Directorate cannot be sure of the physical security employed. Public/external users access this solution from BYOD or non-managed devices. These users do not have privileged access, but the strength of their security controls is unknown.

13 Contingency Planning

13.1 Backup

☒ Backup and recovery requirements of GSUITE-EDU-BS (Sentral component) have been reviewed by the System Manager in accordance with the system's Criticality rating.

13.1.1 Backup model

Describe what is backed up, when, and for how long is it kept	Data (user's and system configurations) within Google is not currently backed up. Deleted data is by default retained by Google for 30 days in a user's recycle bin and an additional 25 days in the system administrators recycle bin. . (https://workspace.google.com/learn-more/security/security-whitepaper/page-6.html) Google cloud applications, Google workspace for Education is backed up to the cloud in real-time so there is no need to remind students to save their work every ten minutes, as used to be the case when working with traditional client word-processing packages for example. The main issue with cloud applications is that every change to the Google Apps data is backed up, even if the student does not intent for it to be saved. While there is the option to return to earlier versions of documents in Google Docs and other apps, there is a limit of 30 days for the deleted files that are stored on Google's server. Any malicious attack on the data of an educational institution causing it to be corrupted, encrypted or deleted will also affect the previously backed up data in the cloud. Google does provide backup for its apps but this is mainly to prevent data loss due to issues at their end such as hardware failures in the data centre. When data is lost due to problems or errors at the user end, they are less likely to be able to help you to restore data. Cloud-to-cloud backup allows you to restore data to a previous stable point in time quickly and easily and also provides robust management tools that allow you to backup and restore all accounts or individual accounts as needed. https://spinbackup.com/blog/google-apps-for-education-backup/

13.2 Google Retention

The current default DDTS retention is: **All backups are retained for 30 days, with fortnightly full capture retained for 52 weeks.** **End of Financial Year (approx. 30 June) and End of Calendar year (approx. 31 Dec) are retained for 7 years.** **What is the retention period for this application, if different?**	Retention policies have been configured in Google Vault to retain data within Google Drive for 2555 days and indefinitely within Gmail. However, data within Vault is only retain whilst the account responsible for creating the data exists within the Google environment. Deletion of the account associated with the data from Active Directory will result in the data being removed from Vault.

13.3 Google System Recovery testing

How often is recovery (from Backup files) tested?	N/A – there is no ability for EDU/DDTS to do system recovery testing of the Google environment. Restoring data from a third-party secure cloud backup service like Google workspace for Education backup by Spinbackup is incredibly fast and easy so there's no need to wait for G Suite administrators to turn up and solve the problem, which eats into teaching and learning time. https://spinbackup.com/blog/google-apps-for-education-backup/

13.4 Google Business Continuity and Disaster Recovery

Is there a documented Business Continuity Plan?	Yes, there is an overarching BCP for the Directorate which includes specific mention of software required for continued school education.
Is there a Disaster Recovery Plan?	Yes, for all the software used and managed by the Directorate. From the service provider please refer to the options - https://cloud.google.com/architecture/dr-scenarios-planning-guide
Date of last review/update?	Information not available.
How often is it exercised/trialled?	Never

14 Configuration Management and Maintenance

14.1 Initial System Configuration

System is already operational at time of this SSP was written.

14.2 Security Configuration

☒	The Vendor configures security settings on behalf of EDU.
☐	EDU configures security settings through configuration console, file or equivalent means.
☒	DDTS ICT configures security settings through configuration console, file or equivalent means. Initial configuration and subsequent changes are performed through the Change Management process.
☒	Other (describe): Please refer to Figure 2 and Figure 3 on user's authentication.

14.3 Major Changes

To comply with the DDTS Change Management process, the Business System Manager must comply with the DDTS *Change Management Policy* and *Change Management Process* (available on DDTS web site). These require the Business System manager to confirm that these procedures are followed for Major Changes (different rules apply for Emergency Changes).

Google is responsible only for changes/updates to the Google product.

The following statements only apply to the SAS software:

☒	Change Owner will prepare (in ServiceNow) a formal Request for Change (RFC) and is responsible for representing the Change at DDTS's Change Management approval meetings: Technical Review and Change Approval Board (CAB). This is for any DDTS supporting infrastructure like ADFS.
☒	DDTS changes have approval before work starts: • for Changes that are being run as projects through the DDTS Program Office, have a Business Requirements Specification (BRS) approved by the business, a Concept Design approved by DDTS, and a Proposal approved by the business. • for Changes that are being run as Business as Usual (BAU) work, have Business approval (the standards for documentation and the Business-side approval to be set by the Business, but as a minimum there must be a document that scopes the change in business terms, and which is signed off by the Business System Manager or his/her delegate) • for both types of Change: have approval from the DDTS CAB to proceed to develop and test the Change ("Rdy4Dev" approval)
☐	Develop and test the Change outside the Production environment, unless there are technical reasons why testing can only be carried out in Production (failure to provide budget for a separate test system does not constitute a valid reason)
☒	The client maintains a Test Plan and Test Cases, and tests to the Plan before UAT certificate is approved: • there is a written list of tests to be run for regression testing • there is a set of standard regression test cases that are run against each new release or bug-fix
☒	Have approval from Technical Review, the prerequisites for which are: • an Operational Readiness Certificate • updated design documentation • an implementation plan
☒	Have approval from the DDTS or EDU CAB to implement the Change into Production ("Rdy4Imp" approval)
☒	Be implemented into Production by DDTS staff. The DDTS Change Management process does not allow the support provider to have access to the DDTS Production server with any elevated privileges.

☒	Education Directorate also have a CAB Process that is applied BEFORE the DDTS process to ensure that all other (non-technical) activities are also in place before the technical change is scheduled.

16.4 Minor Changes

Select all that apply:

☐	**Common process** Minor (Business as Usual) Changes are managed by: 1. DIRECTORATE staff report a problem / request to the DDTS embedded IT team, or to the DDTS Help Desk 2. DDTS raises a ServiceNow case, to act as the formal record 3. An DDTS team member actions the request and records the outcome in the ServiceNow case 4. Minor Changes can result in changes to the Production environment (data correction etc.), as well as to non-Production environments
☐	**Web site** Because of there are fewer than half a dozen staff in the Section, and because the website is simple, the Change Management process reflects that. The process is: 1. A Change to a web page or to content has to be approved by the Business System Manager before the Change is developed 2. The Change to a web page has to be tested by someone other than the person who developed it
☐	**Web site configuration changes** There are no application Configuration changes (including adding new content or amending existing content) that the Directorate's staff can apply. All Configuration Changes are carried out by the DDTS Online Systems team. For content changes: 1. Directorate's staff send the new amended content to the DDTS Online Systems team (in its role of System Administrator / Web Administrator) 2. DDTS Online Systems team raises a ServiceNow case (a Standard Change), to act as the formal record. The DDTS Online Systems team actions the request and records the outcome in the ServiceNow case.
☒	Other (describe): Changes implemented through Google's change management process at Global level solution and for at Enterprise level solution through DSST and DDTS change management process, mostly that comprises of configuration level to meet the business requirements.

15 Vulnerabilities

15.1 Threat sources

A threat source is an individual or group that may seek to cause harm to a system or its data. They are sometimes also known as threat agents or threat actors.

In the context of constructing security risk, threat sources are thought to have a motivation, i.e., why they would seek to harm a system, and a capability, i.e., how effectively are they able to enact this harm.

Threat sources thought to possess the ability to impact the Future State include:

ID	Source	Description	Capability
S01	**Internal users**	Internal staff, including contractors and consultants, with legitimate access to all or part of the organisation's network. As a threat source, staff may have *malicious* (S01A) or *non-malicious* (S01B) motivations. Malicious threats seek to do intentional harm to the organisation and its assets, and intentionally exploit security vulnerabilities to do so. Non-malicious threats are attempting to conduct legitimate business but do so in a way that unintentionally causes harm. In the context of Google, this includes both ACT Government and ACT Education staff, as well as teachers and other school-based positions. Note that students, while technically "internal", are described separately (see *S06*).	**Moderate.** General staff usually have limited and restricted access to information in Google and its data. They will require advanced technical skills and tools to perform an attack.
S02	**Privileged users**	Like *S01*, privileged users are those that have some form of elevated access over the system or its components. As with standard users, privileged users may present a *malicious* (S02A) or *non-malicious* (S02B) source of threat. In the context of Google, privileged users may refer to both business-/application-level administrators, as well as technical administrators (who also largely overlap with *S03*, below).	**High.** Privileged users generally have access to administrative components within a system, coupled with greater technical ability and understanding.
S03	**Service providers**	With Google, administration of the majority of the applications itself, as well as its underlying infrastructure, is performed by the third-party managed service provider Google Pty Ltd.	**High.** Service provider staff have technical skills as well as privileged access to Google Information
S04	**Criminal organisations**	This threat source includes organised, external criminal organisations. Criminal organisations generally exploit IT systems with the intent of monetary gain, e.g., harvesting personal information for sale, or encrypting data to hold to ransom.	**Moderate.** Criminal organisations often have capable technical resources but, in general, prefer to mass-target poorly secured systems rather than pursue a specific organisation.

ID	Source	Description	Capability
S05	**Issue-Motivated Groups (IMGs)**	IMGs are those with ideological or political grievances against the organisation, its mission, or its assets. Some "student activists" may have crossover similarity with IMGs. In the context of this risk assessment, students with legitimate access to Google resources (e.g., current students) are discussed below, as *S06*. In some instances, "insider" students may collude with external IMG resources for a single attack against ACT Education systems.	**Low-Moderate.** IMGs are often persistent but may lack skills or resources. IMGs operating with the collusion of insider threats (see *S01*, *S06*) are likely to have more knowledge and/or access into Education systems.
S06	**Students**	A large portion of the ACT Education network is devoted to serving the ICT requirements of students within the school system. Students are a subset of internal user (see *S01*) and, as such, may be classed as *malicious* (S06A) or *non-malicious* (S06B). As a malicious threat-source, students may be seeking to do damage to teacher or school assets, or to perform data breaches and other compromises (e.g., editing enrolment records). Non-malicious threats launched by students include things such as the spread of malware due to unsafe devices or web browsing, or inadvertent denial-of-service attacks due to poorly configured hardware.	**Moderate.** Students have legitimate access to parts of the Education network, and the potential to gain access to more (e.g., through unsecured teacher workstations). Students may lack skills and resources but are a potentially persistent and motivated threat-source.
S07	**Other cloud tenants**	Within shared cloud resources such as Google, other system tenants may perform actions that impact ACT Education systems, such as the over-consumption of resources (resulting in denial-of-service) or the intentional circumvention of provider security controls.	**Low.** Tenant-to-tenant attacks on the Google platform are exceedingly rare, and the platform itself has its security posture assessed under various national and international standards, including the Australian Government IRAP program See also https://cloud.google.com/security/compliance/irap.
S08	**Parents**	Parents/external agents have access to individual files that have been allowed access to by the information owner It is possible for Parents/external agents with valid access to Google documents to decide to maliciously change or misuse the information.	**Low.** Parents have access to only a very limited set of functionalities in Google and so any malicious damage will be very minimal.

15.2 Key assets

Key assets identified as being relevant to the operation of Google include

ID	Asset	Description	Properties
A01	Organisational reputation	ACT Education and the school system's reputation and public perception. Damage against the organisation's reputation may result in loss of public confidence or business.	☐ Confidentiality ☐ Availability ☐ Integrity ☒ Reputation ☐ Governance
A02	**System certification**	The ability of the system to achieve system certification under relevant accreditation framework, both internal to the organisation and, where required, from external bodies (e g, ASD certification). Inability of the system to achieve certification is generally an indicator that more serious security, governance, or compliance issues exist within its components. This may cause a loss of confidence in the system or organisation.	☐ Confidentiality ☐ Availability ☐ Integrity ☐ Reputation ☒ Governance
A03	**Physical infrastructure**	ACT Education's physical IT infrastructure, including servers, workstations, and network devices. Damage against physical infrastructure includes threats like theft, fire, or other damage that may cause the infrastructure to be unavailable to those systems that require it. In some circumstances, physical damage, such as that to hard disks, may result in data becoming corrupted, impacting system integrity.	☒ Confidentiality ☒ Availability ☒ Integrity ☐ Reputation ☐ Governance
A04	**System infrastructure**	Logical IT infrastructure, such as systems configurations and virtual machines. Threats against system infrastructure include activities such as: • denial of service (DoS) attacks, which exploit bottlenecks in system configurations to impact resource availability. • interception attacks, which attempt to read data while it is in transit or being processed (e.g., read directly from system memory), impacting confidentiality; and • manipulation attacks executed similarly to the above, but with the intent of covertly modifying data and thus impacting integrity.	☒ Confidentiality ☒ Availability ☒ Integrity ☐ Reputation ☐ Governance

ID	Asset	Description	Properties
A05	**Staff and students**	Personnel over whom the organisation has a duty-of-care, including public servants, teachers, students, and contractors. Though unlikely, security threats that impact staff availability are those that cause direct damage to personnel (e.g., physical injury, illness, etc.). Integrity threats may cause to manipulate users to turn against the organisation. Governance threats are the result of the organisation failing to meet legal obligations. An organisation that allows security threats to occur against staff risks being perceived as a poor employer, resulting in damage to reputation. Moreover, the ACT Education system has a duty-of-care to ensure the safety of students, which extends to ICT contexts.	☐ Confidentiality ☒ Availability ☒ Integrity ☐ Reputation ☒ Governance
A06	**Personnel identifying information (PII)**	PII data about organisational staff, students, or members of the public. This may include system data, authentication information (e.g., in Active Directory), and so on. Organisations generally have obligations under the relevant Privacy Act to ensure PII is correct (integrity), available at the request of the individual it identifies (availability), and not released to third parties (confidentiality). Security threats that compromise these requirements may attract legal sanctions (governance), as well as constitute a loss of confidence in the organisation that allows them to occur (reputation). In the context of ACT Education, PII stored about students may have additional legal implications, in that it describes minors and may hold information in relation to health, ethnicity, and similar sensitivities.	☒ Confidentiality ☒ Availability ☒ Integrity ☒ Reputation ☒ Governance

15.3 Vulnerability Assessment

Vulnerability assessment of new systems is built into ACT Government change management processes, and a certificate of acceptance or waiver issued by ICT security is required by ICT Security prior to implementing a system in production.

☐	DDTS Vulnerability Assessment was performed in 2017 (CHG0018062).
☐	Independent Vulnerability Assessment was performed and was approved by ICT Security in [YEAR].
☐	No DDTS Vulnerability Assessment carried out, waiver granted.
☐	No DDTS Vulnerability Assessment carried out, no waiver granted.
☒	Other (describe): Vulnerability testing of the Google infrastructure is conducted by Google. About how Google handles security vulnerabilities - https://about.google/appsecurity/ Google scans all messages to protect against malware, whether or not attachment security settings are turned on. https://support.google.com/a/answer/9157861?hl=en Google Workspace security - https://services.google.com/fh/files/misc/gws_security_whitepaper.pdf

15.4 Vulnerability Management

The procedures used to preserve and check the integrity of the software (including checks for vulnerable software versions and viruses) are:

☒	Vendor managed (describe): Responsibility of Vendor (Google), as a SaaS (Software as a Service) solution.

16 Essential Eight Compliance

Describe how GSUITE-EDU-BS aligns to the ACSC Essential Eight Maturity Model:

Security Strategy	Description	Compliant?	Observation
Application whitelisting Describe how GSUITE-EDU-BS provides application whitelisting for all hosts delivering the solution.	Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g., Windows Script Host, PowerShell and HTA) and installers. Why: All non-approved applications (including malicious code) are prevented from executing.	☐ Yes ☐ No ☒ Partial	Within the Google Ecosystem, Chrome Extensions, Marketplace apps and Android Applications are the functional equivalent of desktop applications. Whitelisting of Chrome Extensions has been enabled for students and Android Applications are currently disabled for both staff and students (except for the ContentKeeper application used for device-based web filtering). Marketplace applications are whitelisted for both staff and students. .
Patch applications Describe how GSUITE-EDU-BS application components are patched for all hosts delivering the solution.	Patch applications e.g., middleware, libraries, plugins. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications. Why: Security vulnerabilities in applications can be used to execute malicious code on systems.	☒ Yes ☐ No ☐ Partial	Service is a SaaS offering accessible only via browser. Services are patched for security vulnerabilities automatically by Google.
Configure Microsoft Office macro settings Describe how any Microsoft Office components associated with GSUITE-EDU-BS are configured to block macros from untrusted sources.	Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. Why: Microsoft Office macros can be used to deliver and execute malicious code on systems.	☒ Yes ☐ No ☐ Partial	Microsoft Office macros are not supported within Google applications.
User application hardening Describe how GSUITE-EDU-BS application components are hardened to reduce the attack surface for all hosts delivering the solution.	User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g., OLE), web browsers and PDF viewers. Why: Flash, ads and Java are popular ways to deliver and execute malicious code on systems.	☐ Yes ☐ No ☒ Partial	Configuration settings for Google have been reviewed as per Google security hardening guidelines. However, a number of key recommendations from external Threat and Risk Assessments around Gmail, and External sharing are being monitored. Progress on mitigating some of the risks is underway
Restrict administrative privileges Describe how administrative privileges have been restricted to the minimum privilege required to perform admin functions, to those with a need to know, and with minimum functionality to perform admin tasks.	Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.	☐ Yes ☐ No ☒ Partial	Administrative rights within Google have been restricted to approved support staff withing SSICT and Education. However, this access is not regularly audited, nor is it linked to any Active Directory as access is granted directly from within the Google Admin console. .
Patch operating systems Describe how GSUITE-EDU-BS operating systems and are patched for all components (hosts, network devices, etc) delivering the solution.	Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions. Why: Security vulnerabilities in operating systems can be used to further the compromise of systems.	☒ Yes ☐ No ☐ Partial	Chromebooks are automatically patched by Google and Windows 10 SOE devices are patched by DDTS ASD on a monthly basis as per the Directorates existing policy.

Security Strategy	Description	Compliant?	Observation
Multi-factor authentication Describe how access to SAS is protected using multiple factors of authentication.	Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high availability) data repository. Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems.	☐ Yes ☒ No ☐ Partial	Whilst MFA is supported it is not currently implemented for either staff or students. Implementation of MFA for students unlikely to be viable given age of students and MFA requirements.
Daily backups Describe how SAS] data and configurations are backed up, retained and restored.	Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes. Why: To ensure information can be accessed again following a cyber security incident (e.g., a ransomware incident).	☐ Yes ☒ No ☐ Partial	Outlined in section on backup and recovery (above) Data within Google is not currently backed up. Deleted data is by default retained by Google for 30 days in a user's recycle bin and an additional 25 days in the system administrators recycle bin. Retention policies have been configured in Google Vault to retain data within Google Drive for 2555 days and indefinitely within Gmail. However, data within Vault is only retain whilst the account responsible for creating the data exists within the Google environment. Deletion of the account associated with the data from Active Directory will result in the data being removed from Vault.

Appendix A: Risk Register

A.1 - DDTS Specific Risks

DDTS provide specific infrastructure to support the operation of Google Workspace – primarily AD FS for user login credentials and access levels authentication (see Figure 7 and 8).

A.2 – Google Specific Risks

Google Workspace is the main teaching and learning system in ACT Government Schools. It is hosted in Google in Australia and is managed by Google Australia Pty Ltd. Google Workspace has links to other ACT Government systems including ADFS for login details (see Figure 1).

Appendix B: Risk Treatment Strategy

The Risks for Google Workplace (defined in Appendix A) and their current treatments have been accepted. No Additional treatments have been listed to address the Risks so there are no additional Treatment Strategies.

Appendix C: Initial Risk Table - Oct 2015

The following table describes treatment strategies for reducing identified risks. The information within the table below can be used to prioritise risk treatment activities as follows:

- High priority treatments are highlighted in **red** and should be actioned within 3 months. These treatments have been determined to provide greater impact for reducing High-level risks.
- Moderate priority treatments are highlighted in **orange** and should be actioned within 6 months. These treatments address Medium-High-level risks.
- Low priority treatments are highlighted in **green** and should be actioned within 12 months. These typically address few risks or have limited impact on reducing the risk levels.

It should be noted that the colours indicate priority in terms of security risk reduction, and do not take into account, resource, cost or business impact.

The 2015 Risks have been included in this newest SSP for completeness. Current risks are listed (above)

Appendix D: Initial Risk treatment strategies for 2015 Risks

The Initial Risk Treatments for the risks identified in 2015 have been included in this new SSP for completeness reasons (to show if all the treatments have been implemented). Current Risk Treatments (identified for this updated SSP in October 2021) are displayed in Appendix B (above).

Appendix E: Risk Methodology

Figure 1: ACTIA ISO 31000:2009 Risk assessment matrix

			Consequence				
			Insignificant	Minor	Moderate	Major	Catastrophic
			1	2	3	4	5
→ Likelihood →	Almost Certain	5	Medium	High	High	Extreme	Extreme
	Likely	4	Medium	Medium	High	High	Extreme
	Possible	3	Low	Medium	Medium	High	Extreme
	Unlikely	2	Low	Medium	Medium	High	High
	Rare	1	Low	Low	Medium	Medium	High

Table 2: Definitions of Likelihood

Level	Description	Detailed Description	Indicative Frequency	Indicative Frequency
5	Almost Certain	Is expected to occur in most circumstances	More than once per year	> 1 in 10
4	Likely	Will probably occur in most circumstances	At least once per 1 year	1 in 10 -100
3	Possible	Might occur at some time	At least once per 3 year	1 in 100 – 1000
2	Unlikely	Could occur at some time (but doubtful)	At least once per 5 year	1 in 1000 – 10,000
1	Rare	May occur only in exceptional circumstances	Less than once per 5 years	1 in 10,000 – 100,000

Table 3: Definitions of Consequence

	Insignificant	Minor	Moderate	Major	Catastrophic
Availability	Interruption to records/data access less than ½ day	Interruption to records/data access ½ to 1 day	Significant interruption (but not permanent loss) to data/records access, lasting 1 day to 1 week	Complete, permanent loss of some clinical/operational records and/or data, or loss of access > 1 week.	Complete, permanent loss of all of a division's clinical/operational records and data.

	Insignificant	Minor	Moderate	Major	Catastrophic
Integrity	Event that may have resulted in the mishandling of clinical or operational records	Inappropriate storage of clinical/operational records in a Branch or Section	Inappropriate destruction/storage of clinical/operational records at the Departmental level	Inappropriate destruction/storage of clinical/operational records, in a public area (inc Internet)	Inappropriate destruction/storage of clinical/operational records, in a public area (inc Internet)
Confidentialit y	Access to individual records by an unauthorised member of clinical or operational staff	Access to individual records by an unauthorised member of non-operational staff	Access to individual records by an unauthorised person from outside the Department	Access to a lot or all of the DB by unauthorised persons. Significant breach of Information Privacy Act	Access to a lot or all of the DB by unauthorised persons. Significant breach of Information Privacy Act

Table 4: Priority for attention

Priority	Suggested timing for treatment	Authority for tolerance of risk
Extreme	Short-term - normally with one month. Detailed action plan required	Director-General
High	Medium term – normally within three months. Needs senior management attention	Senior Executive
Medium	Normally within one year. Specify management responsibility.	Managers
Low	Ongoing control as part of a management system. Manage by routine procedures.	All Staff

Appendix F: Approvals

Certification (endorsement of treatments)

Name of Assessor	Natalie Wise, Anthony Anderson	**Phone**	6207 5563
Name of Certifier	Julian Valtas A/g Chief Information Security Officer (ACT Govt), DDTS ICT Security Telephone: 6207 0073 Email: julian.valtas@act.gov.au		
Certification Decision	☐ CERTIFY – advised risk treatments are EFFECTIVE ☐ DECLINE – advised risk treatments are NOT EFFECTIVE		
Comments			
Signature of Certifier		**Date**	
Name of Endorsee	Jonathan Owen A/g Chief Technology Officer, DDTS Telephone: 6205 3531 Email: jonathan.owen@act.gov.au		
Endorsement Decision	☐ ENDORSE – advised risk treatments protect common assets ☐ DECLINE – advised risk treatments are insufficient to protect common assets		
Comments			
Signature of Endorsee		**Date**	

Accreditation (acceptance of residual risk)

Name of System Manager	Mark Sanderson	**Phone**	6207 5191
Name of System Owner	Kelly Bartlett		

	Executive Branch Manager (Chief Information Officer), EDU Telephone: 6207 5663 Email: Kelly.bartlett@act.gov.au		
Accreditation Decision	☐ ACCEPT advised treatments and residual risk rating of MEDIUM ☐ DECLINE advised treatments and ACCEPT residual risk rating of HIGH		
Comments			
Signature of System Owner		**Date**	

Metadata

Document location:	G:\ICT Security\GRC\Security Assessments\ED\Google)\
Template version:	Vendor Hosted Security Risk Management Plan V5.5
Review cycle:	This SSP should be reviewed every 36 months or when significant changes occur.
Document control:	This is a *controlled* document. Any documents appearing in paper form are not controlled and should be checked against the WIRE version prior to review.

Revisions

Version	Published	Amendment details	Author	Approval
0.0	2/2/2021	First draft – update of 2015 version	R Balla	N/A
0.4	4/11/2021	Review version (changed to new SSP format)	I French	N/A
0.7	27/01/2022	Changes updated	R Balla	NA
1.0	13/4/2022	Minor changes	I French	K Bartlett

STS Safer Technologies for Schools

Prepared by NSIP, a business unit of Education Services Australia for the Safer Technologies for Schools Working Group
Restricted distribution – Distribution is limited to educational jurisdiction chief technology officers, state and territory schools and the service provider listed within this report.

Google Workspace for Education (Google Australia Pty Ltd)

Assessment outcome: Medium risk

The overall risk level is the highest risk level remaining after all available treatments have been applied.

Service summary

Version:	Free – Production	**Review date:**	27/01/2021
Tags:	Collaboration tools; File storage and/or sharing; Classroom management; Digital portfolio; Communication tools; Online meetings / Video conferencing	**Assessment Tier:**	Tier 1
URL:	https://edu.google.com/intl/en_au/	**Audience:**	Staff and Students
Purpose of use:	This service is a suite of in-class productivity tools built for teaching and learning. This review encompasses the following services: Google Gmail, Google Drive, Google Classroom, Google Assignments, Google Calendar, google Jamboard, Google Keep, and Google Sites.		

Information assets and hosting

Data hosting:	Service components (live solution, backup):	Offshore (outside of Australia)	**Data classification:**	☒ Non-personally identifiable information ☒ Personally identifiable information ☐ Sensitive information
	Service provider staff location (support staff):	Onshore (in Australia)		
	Account holder data:	Offshore (outside of Australia)	**Legal jurisdiction:**	California, USA

Parent/carer consent:

Parent/carer consent is required as:

☒ Student personal information is disclosed to register an account*

☒ Student personal information is collected, used or disclosed through use of the service**

☒ Student images, video, work and/or results are uploaded and published to the service**

☐ The service provider requires parent consent for users under 13 yearts to register an account and/or use the service

	☒ Student personal information, including video, audio, or live stream is disclosed through use of the service. * If deidentified information is **not** used. ** if used for this purpose. *Refer to your organisation's policies and procedures to determine consent requirements and the appropriate consent form for this purpose.*
Personal information disclosed through account registration:	• First name (staff, student) • Surname (staff, student)

Additional data disclosed to service:

Personal information

- Works (staff, student)
- Image (staff, student,)
- Video or audio recording (staff, student)
- Phone number (staff)
- Responses - online learning, surveys, forms (staff, student)

Non-Personal information

- Year level (staff, student)
- Class name (staff, student)
- School name (staff, student)
- Country or State/Province (staff, student)
- Responses - online learning, surveys, forms (staff, student)

Additional information:

- This service stores information offshore (i.e., outside of Australia) introducing additional risks beyond those of Australian based providers. For example, stored data is subject to the privacy and security laws of the offshore location rather than Australian laws and may be accessible by foreign governments and citizens.
- Arbitration, mediation, and legal processes are subject to the governing law and jurisdiction of courts in the state or country as set out in the vendor's Terms and Conditions. Where the jurisdiction is outside Australia, Australia's state and federal laws and protections do not apply, and there may be a significant cost to the school/department when entering into these activities.
- This service allows users anonymity or pseudonymity when dealing with the service in some circumstances (i.e., logging support requests using super administrator accounts.
- This service utilises the following products to provide file upload and storage functionality: Google Drive
- Localisation – Prior to use of this service, please contact your educational jurisdiction for any specific requirements or limitations pertaining to this assessment:
  - Government Schools:
    - QLD
    - SA
    - TAS
    - NT

- WA [redacted]
- VIC [redacted]

- Catholic and Independent Schools
  - CEnet / Catholic Education – [redacted]

Terms of Use: https://gsuite.google.com/intl/en/terms/education_terms.html **Privacy Policy:** https://gsuite.google.com/terms/education_privacy.html

Actionable risks and risk treatments

After conducting a comprehensive review, the following risks and associated treatments have been identified. The risk treatments listed are designed to reduce risk exposure. Users must adhere to all stated risk treatments when using this service. The risk level is that which remains after the listed treatments have been applied.

#	**Account management** *Account management standards assess theTerms of Service for the service provider and user, including the data disclosed during account registration, consent requirements, and the policies and processes that apply to account termination, administrator control of accounts and generation of user profiles.*		
	Risk	**Risk treatment**	**Risk level**

PR3
PR4
PR5
	Account registration is required, and the following information must be disclosed:
	• **First name (staff, student)**
	• **Surname (staff, student)**
		• Teachers should register accounts for students using the education options/settings available within the service. When doing so, the information below is disclosed:
		  ○ **First name (staff, student)**
		  ○ **Surname (staff, student)**
		• This service does not require users to enter complete and accurate information when registering accounts. Users should create accounts using anonymous and/or organisational details wherever possible. Complete only mandatory fields.
		• Do not use organisational passwords.
		• Gain consent as per the Parent/carer consent section of this report.
			Medium

PF3	Personal information (e.g., full name, age, DOB, gender, location, contact details, physical description, profile photo) may be stored in or added to user profiles within the service. Users can restrict the visibility of their profile to others to minimise the potential for misuse of personal information and/or identity theft.	• Ensure users do not add any additional information (e.g., full name, profile photo) to their profiles. • Use the functionality available within the service to maintain the privacy of users' profiles by setting to 'private' or only visible to other known users.	**Low**
#	**Usage conditions** *Usage conditions vary based on the functionality available within the service. These conditions aim to reduce the risks associated with student safety, reputational damage, loss of ownership of data, and unauthorised or over-disclosure of personal, sensitive or organisational information.*		
	Risk	**Risk treatment**	**Risk level**
S1	Data in transit is adequately encrypted however, the vendor support some unacceptable protocols.	[redacted]	**Low**
	Forms, surveys and eSignatures *This service offers the following functionality:* • *online forms - customisable / user generated* • *surveys - customisable / user generated* • *sharing of forms/surveys*		
	Risk	**Risk treatment**	**Risk level**

PF5	Use of forms/surveys may result in the unauthorised collection, over collection, storage, and/or disclosure of personal, sensitive and/or organisational information (e.g., when contact information is uploaded for distribution purposes or via responses). Data may be subject to misuse, interference, loss, unauthorised access, or modification. Publishing form or survey links publicly (e.g., online) may elicit inappropriate responses by unknown individuals. Forms/surveys created within this service can be shared as templates for re-use by others. Sharing without implementing adequate controls may result in the unauthorised disclosure of respondents' data.	• When creating forms/surveys: o select or design questions or response fields to limit the collection of personal, sensitive, and organisational information where possible. Use pre-defined response options (e.g., multiple choice, Likert scales) where possible; o oonly collect information that is reasonably necessary to fulfil the purpose of use; o Identify the information classification of the data intended for disclosure/storage within this service. If classified as protected, first seek additional advice/approval from your organisation; o if using this service to collect legally binding information (e.g., consent) with or without electronic signatures, ensure legal advice is sought from your organisation to ensure it is valid and enforceable; and o if using the service to collect updates to school records (e.g., parent contact details, absence), implement an identity verification process (e.g., phoning parents) to validate the change/s. • When distributing forms/surveys: o ensure consent is obtained prior to uploading individuals' contact details for distribution purposes; o only upload personal information that is reasonably necessary to carry out pre-defined functions or activities (e.g., sending to recipients); o use pre-defined recipient lists to restrict the audience as necessary (e.g., class group, parent community, all staff); and o use invitational links or access codes where possible. • When responding to forms/surveys: o provide clear guidelines for students when completing free text fields to ensure they do not disclose sensitive or personal information; and	**Medium**

		○ If sensitive information is inadvertently disclosed, request the service provider to remove the data. • When reviewing/collating and sharing responses to forms/surveys, define and implement school-based business processes to ensure: ○ results are shared on a need-to-know basis; ○ only specific delegates are authorised to send results, preferably using a review and approval process; and ○ proper records management and information handling, including storing records in organisational systems where necessary. • Ensure all existing response data is removed prior to sharing forms/ surveys as templates.	
	Meetings, video conferencing, audio conferencing *This service provides online meetings and/or livestreaming (e.g., video and/or audio conferencing) with the following features:"* • *publicly available sessions* • *private sessions* • *session recordings*		
	Risk	**Risk treatment**	**Risk level**
PF6	Use of this functionality may result in the unintentional or unauthorised disclosure of personal, organisational, or sensitive information; and users' identities and locations being revealed to other participants. Publicly available sessions and/or recordings may result in the unintentional or unauthorised disclosure of personal, organisational, or sensitive information; and users' identities and locations being revealed to other participants and/or members of the public.	• An organisational staff member must be present at all times while users under the age of 18 are participating in online meetings or live streaming (e.g., audio/video conferences). • Keep a record of the conferences in which they participate. Records should include the date, time, and purpose of the conference, and names of participants. • To minimise the personal information that may be disclosed to the public and/or participants without prior knowledge or consent: ○ do not allow students to join the session as registered participants; ○ choose de-identified usernames and/or display names when joining meetings; ○ ensure background noise/conversations are not captured; and ○ do not share or discuss sensitive, organisational, or student information when using this service.	**Medium**

		• If participating in a publicly available conference, ensure participants under the age of 18 are not visible through video feeds, and personal information (e.g., participant name) is not disclosed during audio or within chat messages. • Investigate the moderator controls, publishing of recordings and age appropriateness prior to participation. • Where appropriate, use the functionality available within the service to restrict access to sessions to invited (known) participants only. • Use the functionality available within the service to hide participant details (e.g., de-identify, make private or anonymous). • Use the functionality available within the service to make session recordings private (e.g., restricted to participants only).	
	Screen Sharing *This platform allows meeting hosts and/or meeting participants to use screen sharing with each other. Screen sharing allows other participants to view onscreen files, documents, emails, previews and alerts.*		
	Risk	**Risk treatment**	**Risk level**
PF8	Screen sharing may result in the unintentional disclosure of private or sensitive organisational information. This service does not log screen sharing sessions, so there is limited recourse if used for malicious purposes.	• If screen sharing is required, prevent the unintentional disclosure of private or sensitive organisational information by closing all documents and programs during meetings, including exiting email or communication applications to prevent previews/alerts. Cancel screen sharing as soon as it is no longer required. • Disable participants' ability to share screens with others if not required • Ensure users only share their screen with known users.	**Medium**
	Chat/Instant messaging *This service allows users to engage in chat and instant messaging with the following features:* • *moderation, breach reporting and/or removal* • *administrator controls over user communication*		
	Risk	**Risk treatment**	**Risk level**
PF9	Use of communication and instant messaging may result in the unauthorised disclosure of personal and/or sensitive organisational information.	• Establish protocols and expectations for students when using this functionality. • Report inappropriate communication to the service provider. • Disable the communication tools within this service if not required.	**Low**

		• Restrict communication to known users only (e.g., peers).	
	Commenting and communities/forums *This service provides commenting functionality and/or communities/forums with the following features:* • *Commenting by non-account holders* • *Some moderation, reporting and/or removal features* • *Administrator controls* • *Ability to upload and/or share projects or files in forums/communities*		
	Risk	**Risk treatment**	**Risk level**
PF10	Users may be exposed to inappropriate content or comments and/or cyber bullying through interactions with others. This functionality may also result in the unauthorised disclosure of personal and/or sensitive organisational information. This service allows users to share projects/files in communities/forums. Shared files may be used for malicious purposes (e.g., malicious code, cross site scripting, cross site request forgery). This can lead to malware infection, data and privacy breaches and reputational damage. Further, sharing files may result in the unauthorised disclosure of personal, sensitive, organisational information and/or intellectual property/copyright materials.	• Establish and enforce usage protocols if students engage in commenting. • Ensure commenting is not used by students to communicate with unknown users. • Report inappropriate comments to the service provider. • Use administrator controls to disable commenting or restrict to known users only. Ensure users are aware of the risks of downloading unknown files for both their device and the department's network. • Devices must have antivirus protection installed before downloading executable files from this service. • Users must not upload any material (e.g., written, audio, video) that they do not own or have not created, or any material that infringes Intellectual Property rights such as copyright. • Users must not upload or create content that contains personal (e.g., information that could be used to identify the user, including photos) or sensitive departmental information.	**Low**
	Quiz, poll, flashcard creation and distribution *This service offers the following functionality:* • *Quizzes - customisable / user generated* • *Polls - customisable / user generated*		
	Risk	**Risk treatment**	**Risk level**

PF11	Use of quizzes, polls and/or flashcards may result in the unauthorised collection, over collection, storage, and/or disclosure of personal, sensitive and/or organisational information (e.g., when contact information is uploaded for distribution purposes or via responses). Data may be subject to misuse, interference, loss, unauthorised access, or modification. Publishing quiz, poll and/or flashcard links publicly (e.g., online) may elicit inappropriate responses by unknown individuals. Quizzes, polls and/or flashcards created within this service can be shared as templates for re-use by others. Sharing without implementing adequate controls may result in the unauthorised disclosure of respondents' data.	When creating quizzes, polls and/or flashcards: o select or design questions or response fields to limit the collection of personal, sensitive, and organisational information where possible. Use pre-defined response options (e.g., multiple choice, Likert scales) where possible; o only collect information that is reasonably necessary to fulfil the purpose of use; and o do not use this service to collect protected information. • When distributing quizzes, polls and/or flashcards: o ensure consent is obtained prior to uploading individuals' contact details for distribution purposes; o only upload personal information that is reasonably necessary to carry out pre-defined functions or activities (e.g., sending to recipients); o use pre-defined recipient lists to restrict the audience as necessary (e.g., class group, parent community, all staff); and o use invitational links or access codes where possible. • When responding to quizzes, polls and/or flashcards: o provide clear guidelines for students when completing free text fields to ensure they do not disclose sensitive or personal information; and o if sensitive information is inadvertently disclosed, request the service provider to remove the data. • When reviewing/collating and sharing responses to quizzes, polls and/or flashcards, define and implement school-based business processes to ensure: o results are shared on a need-to-know basis; o only specific delegates are authorised to send results, using a review and approval process where appropriate; and o proper records management and information handling, including storing records in organisational systems where necessary.	**Low**

		• Ensure all existing response data is removed prior to sharing quizzes, polls and/or flashcards as templates.	
	File download *This service allows users to download files. File download functionality has built-in virus scanning and/or malware detection.*		
	Risk	**Risk treatment**	**Risk level**
PF13 PF14	Downloading files from the internet presents a risk to the organisation's network as this increases potential exposure to malicious content or malware. Further, uploading and/or downloading large files may impact your school's bandwidth utilisation which may affect internet speed.	• Ensure users are aware of the risks of downloading unknown files for both their device and the organisation's network. • Prior to downloading any files, ensure devices have anti-virus protection installed. • Refrain from downloading large files during school hours.	**Low**
	Direct email *This service can send, receive and/or store emails.*		
	Risk	**Risk treatment**	**Risk level**
PF15	Storage of communication generated in this service may not meet the organisation's obligations under applicable records legislation.	• Where possible, organisational email communications should be sent using school/work email accounts rather than third party services. • Ensure records that are generated are transferred to an authorised recordkeeping system, as these may need to be retrieved at a later date.	**Medium**
	File upload and storage *This service provides file upload, sharing and/or collaboration functionality with the following features:* • *view and edit permissions* • *administrator controls* *File upload functionality has built-in virus scanning and/or malware detection.*		
	Risk	**Risk treatment**	**Risk level**
PF17 PF18	Accidental, unintentional or malicious sharing of files may result in the unauthorised disclosure of sensitive personal information, intellectual property/copyright materials, and/or organisational information. Further, once intellectual property is shared within this service, users may no longer have ownership of it and/or the ability to prevent the sharing of it.	• Limit the personal and organisational information contained within files and use de-identified information where possible. • Adhere to your organisation's information management procedures. • Ensure users do not upload any material (e.g., written, audio, video) that they do not own or have not created, or any material that infringes Intellectual Property rights such as copyright.	**Medium**

		• Implement a school based business process to ensure users are aware of available file permissions and controls and that these are assigned appropriately. • Disable file sharing if not required.	

Content creation and collaboration

This service provides content creation functionality with the following features:

- *sharing via direct urls*
- *view and edit permissions*
- *administrator controls*
- *publication of user generated content to the service*

	Risk	Risk treatment	Risk level
PF19 PF20	Accidental, unintentional or malicious sharing of content created by users may result in the unauthorised disclosure of sensitive personal information, intellectual property/copyright materials, and/or organisational information. Further, once intellectual property is shared within this service, users may no longer have ownership of it and/or the ability to prevent the sharing of it.	• Limit the personal and organisational information contained within files and use de-identified information where possible. • Adhere to your organisation's information management procedures. • Ensure users do not upload any material (e.g., written, audio, video) that they do not own or have not created, or any material that infringes Intellectual Property rights such as copyright. • Implement a school based business process to ensure users are aware of available permissions and controls and that these are assigned appropriately. • Disable sharing if not required. • Publication of user generated content is opt-in and requires internal approval; determine if publication is appropriate before enabling. • If publishing student work, make students aware and gain specific consent.	**Low**

Content libraries

This service provides content libraries with the following features:

- *template libraries*
- *service provider generated content*
- *some content moderation, reporting and/or removal options*

	Risk	Risk treatment	Risk level
PF21 PF22	No risks have been identified for this functionality due to the limited nature of the functionality and/or controls implemented by the service provider.	• N/A	**N/A**

	Notifications and alerts *This service provides notifications and alerts with the following features:* • *One-way (e.g., broadcast) communication* • *Two-way communication* • *Email communication* • *SMS communication* • *Push notifications*		
	Risk	**Risk treatment**	**Risk level**

PF23
PF24
	User error or failure to manage recipient lists may result in the unauthorised disclosure of personal, sensitive and/or organisational information to unintended recipients (e.g., individuals outside of the school community).	• Schools are responsible for defining and implementing school-based business processes to ensure:
		  o the identities of notification/alert recipients are verified;
		  o notifications/alerts are distributed to the recipients on a need-to-know basis (e.g., messages intended for a single year level are not distributed to the whole parent community);
		  o requests to join subscription lists are validated when requested and reviewed on at least an annual basis and following changes to student enrolment and/or staff employment or role;
		  o notifications/alerts do not contain or request sensitive personal or organisational information; and
		  o only specific delegates are authorised to send notifications/alerts, preferably using a review and approval process.
		• Disable the notification and alert functionality if not required.
		• Limit the audience for each notification/alert on a need to know basis.
		• Manage and regularly review subscriber groups, so only members of the target group receive notifications/alerts.
			Low

Additional service risks

After conducting a comprehensive review, the following service risks have been identified. These risks are inherent within the service itself and cannot be mitigated or controlled by end users, therefore, there are no treatments outlined for these risks.

#	**Protect** *Standards which seek to ensure secure delivery of services. This category includes encryption standards for data at rest or on the move, two factor authentication, physical security (locks, cameras etc.), logging, password and account controls, vendor internal Human Resource (HR) controls (e.g., criminal records checks and HR policies), change management and backup processes.*	
	Risk	**Risk level**
S4	Only logical data segregation is used to isolate or separate customer data which may lead to unintentional exposure of this data to other users.	**Medium**

Information and Disclaimer

Adherence to the usage conditions outlined in this report does not guarantee information security and user safety while using the online service. Users should always exercise caution when using online services and contact their local support teams for assistance if required.

Risk reviews are intended for the internal use of educational jurisdictions and schools only and not intended for external distribution.

If service owners or suppliers are seeking feedback on their review, they may contact [redacted]

Online services are assessed and reviewed to inform and guide schools about the security, information privacy and safety implications of their use.
This report:

- *displays the results of an assessment of online services. The assessment is made based upon criteria agreed by states and territories participating in the Safer Technology for Schools initiative and taken from Australian standards and legislation;*
- *is provided for information purposes only and does not constitute advice;*
- *is dependant upon the accuracy and quality of the information provided by service providers;*
- *is only accurate for the online service at the point in time that the information was provided for the assessment; and*
- *has been compiled by Education Services Australia Limited through its business unit the National School's Interoperability Program (NSIP):*
  - *in good faith. NSIP has endeavoured to ensure that the report is accurate and does not breach any entity's rights at the time of its inclusion. However, the report may contain unintentional errors and is provided 'as is'; and*
  - *on behalf of participating states and territories for the purpose of ensuring consistency in security and privacy and to protect data including the personal information of students.*

Risk assessments evaluate compliance with the Australian Government Information Security Manual and Australian Privacy Principles.

Subsequent changes to an online service and/or relevant information may impact the accuracy of this report. Please inform [redacted] *if any content within this report is inaccurate.*

To the extent lawful, NSIP:

- *excludes all warranties in respect of the report;*
- *is not liable for any loss or damage (direct or indirect) resulting from the use of or the inability to use, the report; and*
- *will not be liable for any incidental, special or consequential damages of any nature arising from the use of or inability to use the report.*

Unless otherwise indicated, the material in this guide is owned by NSIP, a business unit of Education Services Australia, and is subject to the Copyright Act 1968 (Cth). All rights reserved.