Privacy Impact Assessment (PIA) Google Classroom

Brunswick South PRIMARY SCHOOL
imparare insieme • creare insieme • vivere insieme

Information refers to information that is:

- ✓ **personal** (including **unique identifiers** and **re-identifiable** information)
- ✓ **sensitive** (specific characteristics, such as **racial or ethnic** origin, **political** opinions or affiliations, **religious** beliefs or affiliations, **philosophical** beliefs, **sexual** orientation or practices; or **criminal** records) and/or
- ✓ **health** includes behavioural incidents, and opinions about physical or psychological health

Name of Project/Software:	**Google Classroom**		
Project Manager/Staff Responsible *(eg. ICT/Digital Learning/STEM leader)*:	**3 – 6 staff**		
School/Department/Area:	**3 – 6 staff**	Date:	**August 2020**
Email:	**Brunswick.south@education.vic.gov.au**	Phone:	**93801231**
Executive Owner/Principal:	**Trevor Strolla**		

A Privacy Impact Assessment (PIA) considers the privacy impacts of any new or amended project (both school and central-office), process, or software (free or licensed) that handles information.

Completing this PIA template helps you identify key privacy and security risks, evaluate compliance with the Victorian *Privacy and Data Protection Act 2014* and *Health Records Act 2001* (if there is also health information), and document how the risks are mitigated.

When planning to purchase or introduce new software that handles information, especially if they are accessible through the internet or mobile device, doing a PIA should be part of your procurement process.

Instructions

If you need help, contact the Privacy Officer by phone 8668 7967 or email: privacy@edumail.vic.gov.au.

Step

The Project Manager/Staff Responsible should fill in Part 1 (Risk Identification) and Part 2 (Action Plan) of this PIA. See ⓘ for suggested privacy risks to address in the Action Plan. Use the resources in the Appendices to help you complete

Step

- Send the draft PIA template to privacy@edumail.vic.gov.au after a senior school staff or (for Corporate) line manager has reviewed Parts 1 and 2.
- The Privacy Officer will advise if changes are needed or if Part 3 is ready for

Step

- Executive Owner/Principal must review Part 1 and Part 2 before signing Part 3.
- Provide updates to the Privacy Officer until all Action Plan items are completed.
- Keep the signed PIA with other project documentation (e.g. security

Part 1 – Identifying Privacy Risks

Q1. Why do you need a PIA? (select all applicable)

☒ using new software or applications
☐ collecting or handling new information
☐ a change to handling existing information
☐ digitising paper records
☒ new uses for existing software or application
☐ merging, linking, changing datasets with information
☐ using new identification of surveillance methods (e.g. facial recognition, CCTV)
☐ changing to cloud service provider
☐ different cloud service provider
☐ information sharing during stakeholder consultations
☐ Other (provide details): [insert text].

Q2. What functions or activities does this project/software support? (select all applicable) ⓘ Risks: collection; use

- Some apply to **both** school-based and corporate projects. Some are **specific** to schools or corporate only.
- **School-based projects** include projects led centrally but implemented in schools.
- See **Appendix B** for detailed descriptions for functions/activities in a school environment.

Teaching and Learning

☐ Academic Assessment & Reporting
☒ Education – Curriculum Planning and Activities
☒ Education – Individualised Planning

Communication and Engagement

☐ Parent Portal - Interactive or Self-Service
☐ School one-way communications – Bulk
☐ School one-way communications – Specific
☐ Visitor Registration System

Student Administration

☐ Attendance
☐ Calendar
☐ Events Management
☐ Health and Wellbeing [WKL1]- Behavioural Management (excludes health information)
☐ Health and Wellbeing – Support for Special Needs or At Risk Students
☐ Timetabling

School/Corporate Administration and Management

☐ Device Management Software
☐ Employee/Staff Timecard
☐ Finance Management – Budgets and Reporting
☐ Finance Management - Accounting
☐ Finance Management - Online Payment Systems
☐ Information Sharing Arrangements
☐ Library Management System
☐ Monitor and Reporting - Department Services
☐ Ordering Systems - Canteen, Books, Uniform etc
☐ Online Administration Forms and Surveys
☐ Print Control Technology
☐ Referral System
☐ Records Management System - Administration
☐ Statistical Research and Analysis
☐ Staff Performance & Evaluation
☐ Service Delivery Allocation- Department Services
☐ Workflow Management System

If there are **any other or additional** functions/activities, please **also** specify:

Students have the ability to store and share any school work related content on the platform, such as photographs, audio, video recordings. They can also add non-classroom related information.

Q3. What improvements will this project/software deliver and what are its benefits (e.g. for schools, parents, students, DET)?

Currently, Victorian government schools continue to adopt and use a range of Information and Communication Technology (ICT) to improve learning and teaching at an accelerated rate. Schools are actively turning to cloud based offerings as students have different types of devices (such as tablets and/or laptops) and these services can provide uninterrupted 24/7 access.

This school is facilitating the installation of G Suite on school, students and teachers devices. The expected benefits for the availability G Suite for this school include:

- Allowing students to actively collaborate on school work and activities
- Providing storage space
- Allowing staff to contribute, collaborate and access key school documents

- Allow staff and students to access documents/files off-site
- Teaches students to be 'digital citizens' through the use of an online system.
- Provides access to digital tools for a range of classroom activities.
- Allows students to actively collaborate with their class on school work.
- Provides digital whiteboard capability in group discussions.
- Enables students to access their classwork from different channels (i.e. laptops, iPads and smartphones).
- Helps students to build working relationships with each other.
- Promotes knowledge sharing by staff

Teaching students about the importance of privacy can prevent identity fraud and other crimes. Through communicating the importance of privacy to students, schools can educate them on:
APPROPRIATE USE – ensuring that online tools are being used appropriately for learning
LIMITING SHARING – limiting the collection of personal and sensitive information from students
BEING SAFE – informing teachers of any concerns when using online tools

Utilising cloud services will also allow the school to direct resources away from hardware maintenance to programs/projects that support teaching and learning activities

Q4. Does this involve other Department, school or other agency (e.g. VCAA) datasets? (Select all applicable)
ⓘ Risks: *data quality, unauthorised access*

☒ No
☐ Access/import.
Student accounts are created following an export of student data from CASES21
☐ Write-back/synced/exported back to other datasets
Student accounts are created and then continually updated with data from CASES21
☐ Yes, Other. Details of the kind of interaction and what data sets: insert text *e.g. NAPLAN data and Lookout dataset is linked to the VSN.*

Q5. Who is involved, their roles, what they will do and what information they can access?
(For Corporate – modify this accordingly)
ⓘ Risks: *collection, use & disclosure, unauthorised access*

☒ Students [# e.g. 300]	Account: Student	Access: • personal files • assigned classwork • work produced by other students/teachers shared directly with them • files shared with all members of the set groups (classes, student groupings)
☒ Teachers [#]	Account: Teacher	Access[WKL2]: • personal files • student files shared with teachers (students are requested to have files saved in "team Drive" with access to relevant staff • classwork • work produced by other students/teachers shared directly with them

- files shared with all members of the set groups (classes, student groupings)
- curriculum planning files
- Student assessment files

☒ Parents	Account: no account	Parents do not have direct access to this service
☐ Others: [3] School Technician, School coordinator (ICT Leader)	Account: Administrator	Access: Full access to create and manage users.

☐ [insert text].	[insert text].	[insert text].

Q6. Fill out this information table [see **Appendix B** for typical information for common school functions/activities] The first 3 rows are examples only. Please **delete and fill out** based on the relevant project/software.

Whose and what information	*Is it personal, health or sensitive information?*	*Is this new information that you did not collect previously, or existing information that you already have?*	*Usage (see e.gs. of primary purposes in School's privacy policy or DET Information Privacy Policy)*	*Where will it be stored?* *(if unsure, email the supplier)*
First name + family name of student	*personal*	*Existing*	*enable teachers to identify and give feedback to individual students*	*Student's data is stored in data centers located in the USA, Chile, Taiwan, Singapore, Ireland, Netherlands, Finland and Belgium.*
Students' Year level and class	*n/a*	*Existing*	*Enable teachers to identify appropriate curriculum activities for student learning*	*Same as above*
Student CASES21 code	*Personal*	*Existing*	*Allow for the accurate identification of students*	*Same as above*
Photos/video of student engaging in tasks	*personal*	*New*	• *Enable school to communicate with parents about student learning activities* • *Assessment and reporting evidence* • *Presentation of class work*	*Same as above*
Student class work – may contain sensitive information	*personal*	*New*	• *Enable school to communicate with parents about student learning activities* • *Assessment and reporting evidence* • *Presentation of class work*	*Same as above*
Location information and preferred language	*personal*	*New*	*Google collects information based on the use their services.*	*Same as above*

Wellbeing information			• *support students' social and emotional wellbeing, and health*
			• *fulfil legal requirements, including to:*
			  ○ *take reasonable steps to reduce the risk of reasonably foreseeable harm to students, staff and visitors (duty of care)*
			  ○ *make reasonable adjustments for students with disabilities (anti discrimination law)*	

			○ *provide a safe and secure workplace (occupational health and safety law)*	

Google Apps services do not collect or use student personal information and data for advertising purposes or to create advertising profiles.

Q7. Any other matters that you consider may become privacy or related information handling risks?
ⓘ **Risks:** *insufficient notice of collection (Q9), unexpected use (Q12), unauthorised access (Q19), e-safety, copyright*

☐ Remote access function
☒ Unmoderated or unsupervised chat/communication functions
☐ Video or teleconferencing function
☒ Accessible on portable devices
☐ Users can share content publicly (including copyrighted works or student works)
☒ Students/staff sign-in using their personal accounts on social networking services (e.g. Google, Facebook)
☐ Other risk(s). Please provide details:

Questions 8 to 20 are aligned against the Information Privacy Principles (IPPs) (see IPP summary in **Appendix A**). Give details of **existing** controls or processes where requested in Part 1. **Proposed** steps should be in the Part 2 Action Plan.

Cetion (IPP 1), Use (IPP2) & Sensitive Information (IPP 10)

Q8 If you are collecting new information and/or using existing information, can you proceed with the project without any of it?	☒ No, all information collected or used is necessary. • The school has a policy and processes for the handling and use of student images. • Students will also be encouraged use the service for school related tasks (see School acceptable use policy). However, given the nature of the 'online services' provided by G Suite for Education, there is potential for students to store information in the applications that are non-classroom related and health information which could be include one or more categories of health information as described above. • Staff will ensure that any student information collected and stored in the system complies with agreed school protocols. ☐ Yes. ⓘ **Address risk in Action Plan:** *unnecessary information collected or used*

Q9 Do you have processes to notify parents and/or relevant individuals (whichever are applicable) about the collection and use of new information? *Required details to include in the notice* *a) Name of organisation collecting the information (if external to DET/School) and contact details;* *b) The fact that the individual is able to gain access to the information; and* *c) The purposes for which the information is collected; and* *d) To whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and* *e) Any law that requires the particular information to be collected; and* f) *The main consequences (if any) for the individual if all or part of the information is not provided.*	☐ No. ⓘ **Address risk in Action Plan:** *inadequate notice* ☐ No notice is required because the information is collected indirectly and notification would result in serious threat to life/health. ☒ Yes. The school has provided information packs on G Suite for Education to parents. These include the following information: • What is G Suite for Education and its current 'online services' offerings • Benefits in the classroom by using G Suite for Education • Protecting student information – providing parents on privacy risks (inc. information may be collected due to any legislation), mitigation strategies and how can parents protect their children • What information is being collected and provided to Google and purpose for the collection • What information students should not be input to G Suite for Education (such as health information or other personally identifiable information) • Data lifecycle in G Suite for Education (inc. where data may be held outside Australia) – how information is: collected, used, secured, destroyed, disclosed • Links to Google's Agreement and privacy for G Suite for Education • Ability for parents to provide opt-out consent to using G Suite for Educational The G Suite information pack will also be made available to parents online ☐ Some. ⓘ **Address risk in Action Plan (if applicable):** *inadequate notice* Details of how and when you provide the required details: [insert text].
Q10 If you are collecting new health or sensitive information (see Q6), have you considered if consent is required? *Valid consent must be: voluntary, informed, specific and current.*	☐ Not Applicable, not collecting new health or sensitive information. ☐ Consent is required. ⓘ **Address risk in Action Plan:** *invalid consent* Reason: [insert text]. *E.g. collecting sensitive or health information and no other exception applies* ☒ Consent is not required. Reason: The school has provided parents with an information pack which details the use of the application for schoolwork and the circumstances in which information may be disclosed. Within the information pack, parents have the opportunity to opt-out their child from the use of the application. Due to the nature of the information pack and opt-out process, there will be an informed consent on the disclosure of the information stored within the services.

Use And Disclosure (IPP 2), Anonymity (IPP 8), Unique Identifiers (IPP 7), & Transborder Flows (IPP 9)

Q11 When using existing information identified in Q6, do the purposes in the original notice given during the earlier collection, permit or relate to the proposed use in this project/ software?	☐ Not applicable, only new information being used/disclosed. ☐ No. ⓘ **Address risk in Action Plan:** *inadequate notice for secondary use* ☒ Yes. The use and disclosure of existing information to Google is to assist with the delivery of teaching and learning programs. This is consistent with the primary purpose of collection.

Q12 Would parents/individuals reasonably expect you to use the existing information for the proposed use/disclosure in this project/software? *E.g. disclosure to new ICT supplier, marketing, selling information*	☐ Not applicable, only new information being used/disclosed. ☐ No. ⓘ **Address risk in Action Plan:** *unexpected use/disclosure* ☒ Yes. The use and disclosure of information to Google is to assist with the delivery of teaching and learning programs. This is consistent with the primary purpose of collection. Parents are also notified of the use of online tools when the personal information is/was initially collected.
Q13 Based on your response in Q5 about who has access, is access limited to the information each party needs to know in order to carry out their roles?	☐ No. ⓘ **Address risk in Action Plan:** *excessive disclosure* ☒ Yes, There are legal, technical and behavioural measures in place, including applied access permissions and contract terms requiring ICT supplier to not access the data without consent. Staff have received appropriate training and have an agreed (and documented) understanding of how the system is to be used. The school has provided parents with clear advice on the use G Suite for Education and privacy information packs on G Suite for Education. In addition, within the G Suite for Education Privacy Notice, Google has stated that they will not share personal information with companies, organisation and individuals outside of google, unless: • There is user consent • The individual is a g Suite for Education administrator (these individual will be school administrators) • external processing with affiliates and trusted business partners (these parties are bound by the Google Privacy Policy, and other appropriate confidentiality and security measures) • For legal reasons.
Q14 Based on your response in Q6, if you are using unique identifiers, are you using them only when permitted? *E.g. VSN, CASES21 ID, Medicare number. Use of VSN is strictly regulated and VCAA approval is required. If this identifier is needed, may consider using CASES instead of VSN.*	☐ Not applicable, not using unique identifiers. ☐ No. ⓘ **Address risk in Action Plan:** *unpermitted use of unique identifiers* ☒ Yes. The use of the CASES21 student code is necessary to allow for accurate student identification

Q15 Based on your response in Q6 about whether the information is stored or accessed from outside Victoria (e.g. on the cloud with servers outside Victoria, or overseas technical support), have you done any of the following to protect it? a) *the parties outside Victoria have represented that they will apply similar protections* b) *Have a contract to ensure similar protections to Victoria apply; or* c) *Get consent from the parents/individuals; or* d) *Transfer is necessary for performance of a contract and for the individual's benefit*	☐ Not applicable because data is not stored or accessed from outside Victoria. ☐ No. ⓘ **Address risk in Action Plan:** *unprotected transborder data flow, no contract in place that addresses data security and retention requirements and data migration in case of change in cloud provider.* ☒ Yes. The school has provided information packs to parents highlighting that Google will store information outside of Victoria. Student's data is stored in data centres located in the USA, Chile, Taiwan, Singapore, Ireland, Netherlands, Finland and Belgium. Parents will have the opportunity to opt-out of the use of the service based on any transborder data flow concerns. As Google operates in a wide geographical region, they have chosen to adopt the US privacy requirements as the baseline form of privacy requirements. As stated in their support page: • G Suite for Education complies with the U.S. Family Educational Rights and Privacy Act (FERPA), and our commitment to do so is included in our agreements. We contractually require G Suite for Education schools to obtain parental consent regarding the use of our service in conformity with the U.S. Child Online Privacy Protection Act (COPPA), which facilitates compliance with COPPA requirements. • Furthermore, to be able to comply with the European data protection requirements, Google has provided compliance options to address the EU data protection regulations. Refer to the following link for further information: https://support.google.com/googlecloud/answer/6056694
Q16 Must individuals be identifiable (i.e. not anonymous) during this project or when using this software?	☐ No, anonymity is possible. ⓘ **Address risk in Action Plan:** *information is not anonymous* Details of how information is anonymised: [insert text]. ☒ Yes, anonymity is not possible for this project or software.
Q17 If aggregating or de-identifying information, is there an existing process to reduce the risk of being re-identified or linked to other data that re-identifies?	☒ Not Applicable. ☐ No ⓘ **Address risk in Action Plan:** *re-identification* ☐ Yes. Details of process in place: [insert text]. *E.g. aggregated reports are for internal school/Department use only.*

Data Quality (IPP 3), Access and Correction (IPP 6)	
Q18 Is there an existing process in place to reasonably ensure information collected is accurate, complete, and up to date?	☐ No. ⓘ **Address risks in Action Plan:** • *harm resulting from decisions informed by inaccurate data* • *accidental disclosure due to incorrect contact details* ☒ Yes. The school system administrator will regularly review all school accounts. The school will use a software tool to regularly compare student enrolment data from CASES21 to Google student accounts. This will allow for accounts to be created and suspended appropriately. Teachers will continually review student accounts for accurately. Staff accounts will be reviewed each term and also modified to reflect any known staffing changes.
Data Security (IPP 4)	
Q19 Have you taken reasonable steps to protect information from misuse, loss, unauthorised access or modification? *Reasonable steps may include: logging IT service desk request for a data security assessment of applications using Edupass login (for schools) or of the ICT supplier(for corporate projects)*	☐ No. ⓘ **Address risks in Action Plan:** ☒ Yes. School process adhere to DET security policies. • *Ensure all portable devices are suitably secure (see DET policy)* • *access revoked promptly when no longer required* • *access restricted to unauthorised staff or 3rd parties* • *Appropriate training provided to all staff* • *staff/students agree to acceptable use policy* • *information encrypted* • *software has appropriate access/audit logs* • *Administrator and staff accounts have 2 factor authentication*
Q20 Does your activity have processes that comply with the DET's data retention and disposal requirements (Schools and Corporate)? *An existing Retention & Disposal Authority (RDA) may apply. Contact archives.records@edumail.vic.gov.au* *See list of common temporary records and permanent records. RDA for School Records (PROS 01/01) is currently being revised, which may affect retention period for health and wellbeing records.*	☐ No. ⓘ **Address risks in Action Plan:** • *information kept longer than required retention period* • *information destroyed before retention period is over* • *no requirement for ICT supplier to delete and return information after contract is over or at DET/school's direction* ☒ Yes. • Information is not kept longer than required retention period • information destroyed in line with appropriate retention period • ICT supplier to delete and return information after contract is over or at DET/school's direction **PROS 01/01 VAR 8 Retention and Disposal Authority for Records of School Records Issued Date: 20/08/2018** https://prov.vic.gov.au/sites/default/files/files/documents/0101var8.pdf

Part 2 – PRIVACY COMPLIANCE ACTION PLAN

Please review your responses in Part 1, and using the table below, specify actions required to mitigate identified privacy compliance risks.
*Use the Consequence Criteria and Likelihood Criteria in **Appendix C** to determine the pre-action Risk Rating.*

	Identified Privacy Risk **Suggestions are not exhaustive, amend/add/delete to ensure risks are relevant for your school or project*	Risk Rating *based on existing controls in Part 1*	Action Required *Some suggested actions below, not all are relevant. Amend as needed. Suggestions are not exhaustive.*	Responsible Person/Area	Timeframes
1.	More information is collected, used or disclosed that is necessary (Q5/Q6/Q7/Q8/Q13/Q14)	Consequence: Choose an item. Likelihood: Choose an item. Risk Rating: Choose an item.	• Teachers develop and agree on protocols for the storage and use of student information • No use of student photos as avatars • Senior staff member reviews all student records on regular basis to ensure accuracy and adherence to school agreed protocols	• ICT / Welfare coordinator • Assistant Principal	• Prior to any student teacher comments being included • Weekly
~~2.~~	~~Unexpected use: ICT supplier uses information for marketing or other purposes without consent or de-identification (Q5/Q7/Q12/Q13)~~	~~Consequence: Choose an item.~~ ~~Likelihood: Choose an item.~~ ~~Risk Rating: Choose an item.~~	~~Use DET template contract with ICT supplier or ensure T&Cs include model terms~~	~~[insert text].~~	~~[insert text].~~
~~3.~~	Unauthorised access: Staff changing roles that no longer require them to access the information (Q13/Q18/ Q19)	Consequence: Choose an item. Likelihood: Choose an item. Risk Rating: Choose an item.	Regular review of teacher accounts (each term and when advised of role changes)	[insert text].	[insert text].
4.	~~Data will be accessed and/or transferred outside Victoria without similar protections (Q6/ Q15)~~	~~Consequence: Choose an item.~~ ~~Likelihood: Choose an item.~~ ~~Risk Rating: Choose an item.~~	~~1. Use DET template contract or ensure T&Cs include model terms~~ ~~Risk partly accepted for no vendor contract during pilot because opt-in consent sought from parents prior to implementation and overall risk is low due to likelihood and severity of harm due to the limited personal information collected.~~	~~[insert text].~~	~~[insert text].~~

~~5.~~	Inadequate process to ensure information is kept up to date (Q5/ Q18)	Consequence: Choose an item. Likelihood: Choose an item. Risk Rating: Choose an item.	School coordinator to review user account on a regular basis. Software tool (user creator) to be used to ensure student user accounts are up-to-date	[insert text].	[insert text].
6.	Misuse and unauthorised disclosure of information by staff (Q19)	Consequence: Choose an item. Likelihood: Choose an item. Risk Rating: Choose an item.	1. Staff to be trained and provided with guidelines regarding Schools Privacy Policy. 2. Staff to be trained in how to upload material and use the software 3. Create access protocol which includes managing access requests and a Register of access requests and changes 4. Communication plan and staff training to be developed to minimise risks of misuse and maximise benefits Staff accounts use 2 Factor authentication	[insert text].	Annually
7.	Misuse and unauthorised access by students and parents (Q5/Q7/Q19)	Consequence: Choose an item. Likelihood: Choose an item. Risk Rating: Choose an item.	1. Staff accounts use 2 Factor authentication 2. Inform parents and students about expectations of acceptable use and what information should not be posted/ uploaded: e.g. personal mobile or phone numbers, personal photographs and videos unrelated to school work 3. Ensure all communications are moderated 4. Establish a process to regularly monitor all information posted and uploaded	[insert text].	[insert text].
8.	Unauthorised access through portable devices (Q7/Q19)	Consequence: Choose an item. Likelihood: Choose an item. Risk Rating: Choose an item.	1. Ensure compliance with DET Portable Storage Device Security Policy 2. Ensure staff and TSSP are aware of DET Portable Storage Device Policy – raised during staff meeting/ email reminder from principal 3. Password protection in portable devices 4. Staff accounts use Two-factor authentication 1.	[insert text].	[insert text].
9.	Unauthorised access of accounts due to insecure passwords (Q7/Q19)	Consequence: Choose an item. Likelihood: Choose an item. Risk Rating:	1. All staff, students and authorised users are notified of DET password policy principles. Staff accounts use 2 Factor authentication 2. Ensure that password controls are implemented that comply with the DET password policy	eLearning/ICT coordinator School Technician	[insert text].

		Choose an item.	3. No generic log ins are used 4. Two-factor authentication 5. Use of password management applications		
10.	Privacy risks not adequately mitigated because of project change or actions in Part 2 are not implemented.	Consequence: Major Likelihood: Possible Risk Rating: High	1. Provide regular updates on status of action items to Privacy Officer until items are completed (If necessary) Do annual review of project/current activity to see if updated assessment is required	Project Manager/ Responsible Staff	1.Updates at the end of each of the timeframes set out in Part 2 2.annually
11.			2.		

Part 3 – ENDORSEMENT OF PRIVACY IMPACT ASSESSMENT

Project Manager/Responsible Staff Declaration			
I acknowledge Department's obligations to comply with the Privacy and Data Protection Act 2014 (Vic) and DET's Information Privacy Policy. *This Privacy Impact Assessment has been completed in good faith and the responses provided are true and correct to the best of my knowledge. All action items identified in Part 2 of this document will be implemented as part of the project/activity plan.* *The privacy impacts of this project/activity will be reviewed periodically or whenever there is a change that may impact on privacy and any additional privacy risks identified throughout the project/activity will be addressed with appropriate action.* *I will provide regular updates to the Privacy Officer on the action items at the end of each of the timeframes set out in Part 2.*			
Name:		Title:	
Signature:		Date:	

Executive Business Owner/Principal (Sponsor) Endorsement			
I acknowledge and accept the risks and associated actions required as outlined in this document.			
Name:		Title:	
Signature:		Date:	

*Principals can consider whether to share the completed PIA with the school council

Privacy Officer Certification			
I certify that this PIA has been completed in accordance with DET policy and process. This certification is conditional on: • *all relevant information having been provided by the Project Manager; and* • *completion of all action items identified in Part 2 of this document.*			
Name:		Title:	
Signature:		Date:	

Appendices - Resources

Useful links to privacy resources

- DET Information Privacy Policy; Data Protection Act 2014 Schedule 1;
- For schools: Online privacy pages for schools and Schools Privacy Policy
- Office of the Australian Information Commissioner: Guide to Privacy Impact Assessments
- Alternatively at minimum, require vendors to insert the following on their tax invoices: [Suggested wording]
  The supplier issuing this invoice agrees to comply with the obligations of a contracted service provider under section 17(2) of the Privacy and Data Protection Act 2014 (Vic) and section 12(1) of the Health Records Act 2001 (Vic) in the course of its provision of the invoiced goods or services to the school council. The supplier also agrees to assist the school council to comply with its legal obligations by following the school council's directions to the fullest extent possible.
- Where moving to a new or different cloud service provider,

Other relevant policies or frameworks

Consider whether there are any relevant policies or frameworks with information handling requirements that you may also need to comply as a result of this project or the software. For example:

IT

- SPAG IT Policies: CASES21, ICT Supply, Acceptable use of ICT resources
- SPAG: Use of Digital Technologies Resources
- School: Acceptable Use Agreements (for students)
- Department: Password Policy
- Corporate and schools: ICT Acceptable Use Policy
- Department: Portable Storage Devices Security Policy (for staff personal devices)

Procurement

- Corporate and Schools: Procurement policy and procedure
- For schools: contact the school procurement team at schools.procurement@edumail.vic.gov.au for which Department contract templates to use based on the risk levels
  1. School Council Purchase Order Terms and Conditions - Goods and Services up to $2,500 (lower risk)
  2. School Council Short Form Services Contract (lower to medium risk)
  3. School Council Agreement for the Provision of Services (higher risk)
- For corporate: use the Corporate Procurement portal or use the Ariba helpdesk via the IT Service Gateway

Copyright and Privacy

- Educational licences
- Copyright Guidance, Copyright Release Guidelines
- Copyright permission to publish students' works online
- Photographing and Filming Students Policy and consent forms

Other

- ETRA requirements: VCAA approval for use of VSN. If you are using or are intending to use the VSN or information from the VSR, you need to seek advice from the VCAA. For further information, please contact: James Bradlow, Special Project Manager – Victorian Student Number, VCAA on 03 9032 1745 or bradlow.james.e@edumail.vic.gov.au
- Department Risk Management Framework: Schools and Corporate

Click on the following links:

Appendix A: Summary of Information Privacy Principles
Appendix B: Key Considerations for Common School Functions
Appendix C: Department Risk Management Framework: Consequences Criteria, Likelihood Criteria, Risk Rating, Acceptability Chart

Appendix A: Summary of Information Privacy Principles

IPP 1 Collection

- You must only collect personal information that is necessary for the performance of your function.
- You must tell individuals why you are collecting their personal information and how they can update or correct their personal information.

IPP 2 Use and Disclosure

- You can only use and disclose personal information in accordance with the primary purpose it was collected for or for a related secondary purpose that a person would reasonably expect.
- In the case of sensitive information (see IPP 10, below), it must be directly related to the primary purpose of collection.
- Generally, if a use or disclosure would not be reasonably expected, you should seek consent.
- There are some exceptions where the use or disclosure is required by law, for the public interest or an individual's health and safety.

IPP 3 Data Quality

- You must take reasonable steps to ensure individuals' personal information is accurate, complete and up-to-date.
- You must take reasonable steps to protect individuals' personal information from misuse, loss, unauthorised access, modification or disclosure.

IPP 4 Data Security

- Personal information is to be permanently de-identified or destroyed when it is no longer needed for any purpose.
- Ensure the security of information and its proper storage, archiving or disposal in accordance with appropriate recordkeeping standards and information technology safeguards.

IPP 5 Openness

Organisations must have a document that clearly explains how it manages personal information. This document is usually called a 'privacy policy' and must be provided to anyone who requests it.

IPP 6 Access and correction

Individuals have a right to seek access to their personal information and to make corrections, subject to limited exceptions (e.g. if access would threaten the life or health of an individual). Access and correction rights are mainly handled by the *Freedom of Information Act 1982* (Vic).

IPP 7 Unique Identifiers

You and the Department cannot adopt or share unique identifiers (i.e. a number or other code associated with an individual's name, such as a driver's licence number) except in certain circumstances, such as where the adoption of a unique identifier is necessary for you or the Department to carry out one of its functions, or by consent.

IPP 8 Anonymity

If it is lawful and feasible, you must give individuals the option of not identifying themselves (i.e. remaining anonymous) when they engage with the Department.

IPP 9 Transborder data flows

Organisations may only transfer information (health or personal) to someone outside of Victoria where the recipient of the information is subject to similar privacy laws. The privacy rights an individual has in Victoria remain, despite the information being transferred to another jurisdiction.

IPP 10 Sensitive information

You can only collect sensitive information in restricted circumstances, or by consent.

Appendix B: Key Considerations for Common School Functions

RDA suggestions are suggestions only, based on the current RDA for School Records (PROS 01/01) which is in the process of being revised. Please contact Records team at archives.records@edumail.vic.gov.au for records advice.

Teaching and Learning

Academic Assessment & Reporting

Records assessment, NAPLAN, awards and standardised testing results and used to produce a student profile and reporting based on individual, progression or whole of school profile.

Information: Student name, year level, DOB, VSN (only if needed for reporting on NAPLAN), CASES21, attendance or absentee code/reason, attendance comment, student assessment details including special consideration and comments, family contact details: Name, email address, work and home address, phone

Access: usually principal, assistant principal (AP), leadership team, data coordinators and teachers, (view only) parents and students

RDA suggestions: Prep to Year 8 reports (6 years after departure), Year 9 to 12 reports (30 years after departure), Summary Enrolments records are permanent.

Education – Curriculum Planning and Activities

To plan lessons and deliver classroom activities and homework, either on classroom-level, year level or subject basis. Programs delivering curriculum to students, facilitating student learning and interaction, including online and digital learning. May be subject-specific such as mathematics or English applications. May feed into Academic Assessment and Reporting and School Communications – one way

Information: Student name, year level, email, teacher name and email. assessment result for in-class activities, quizzes, homework, teacher name and email. **Consider carefully if using CASES21**

Access: usually principal, AP, teachers, educational support staff, students

RDA suggestions: Teacher work books (after admin use), Student reference records (1 year after departure)

Education – Individualised Planning

To plan lessons, classroom activities and homework, or facilitate student learning and interaction on an individual student basis, for at risk students or students with special needs.

Information: Student name, year level, email, teacher name and email. Consider carefully if using CASES21 or special comments.

Access: usually principal, AP, teachers, educational support staff, students

RDA suggestions: Student reference records (1 year after departure), teacher work books (after admin use)

Communication and Engagement

Parent Portal - Interactive or Self-Service

A portal which allows parents, carers or guardians to manage student information, access online school services, manage payments, provide consent or approval. This often links with other school functions e.g. School one-way communications – Bulk, School one-way communications – Specific, Attendance, Assessment Reporting, Calendar

Information: Student name, year level, additional notes about students to parents, family contact details including contact flag, teacher name and email, and other Information depending on other functions.

Access: usually principal, AP, admin, leadership team, teachers, parents

RDA suggestions: parental notes (1 year), student reference records (1 year after departure)

School one-way communications – Bulk

Bulk general communication via notices, broadcasts, newsletters and alerts from schools to parents/carers/ guardians. This could be done by sms (including bulk sms), email or mail. This system may also draft and publish or email the bulk communications.

Information: Student name, year level, teacher name and email (if applicable), family contact details including whether speaks English at home.

Access: usually principal, AP, admin staff, leadership team, teachers (create not publish), (view only) parents and students

RDA Suggestions: Operational correspondence (7 years)

School one-way communications – Specific

Specific communications to families about individual students. Often used to provide updates to parents about their specific child's education outcomes, homework and classroom activities.

Information: Student name, year level, email, student assessment results for in class activities, quizzes and homework, notes/communications to families, teacher name and email, family contact information **Consider carefully if using CASES21 or student photos**

Access: usually principal, AP, teachers, (view only) students and parents
RDA suggestions: Student reference records (1 year after departure), Operational correspondence (7 years)

Visitor Registration System

Records sign-in & sign-out of visitors, contractors and anyone else coming on school property. System may be used for safety and emergency management.
Information: Visitor name, contact information, reason for visit, who visiting/supervising. **Consider carefully if includes: Working with Children Check (how is it recorded)**
Access: usually principal, AP, admin, leadership team, teachers, OHS rep, parents, students, visitors
RDA suggestions: destroyed after admin use concluded. Require ICT supplier to delete information at school's direction.

Student Administration

Attendance

To record student attendance and any absences at school and in classes. It also notifies parents within same day that their child is absent and records a reason for the absence.
Information: Student name, year level, DOB, attendance or absentee code/reason, attendance comment, family contact details: Name, email address, work address, home address, phone numbers, contact flag. **Consider carefully if: student photograph**
Access: usually principal, AP, leadership team, student welfare coordinators, admin staff, teachers, parents
RDA suggestions: Attendance records (6 years after departure).

Calendar

To communicate excursions, exam periods, curriculum and student-free days or other school planning. Can offer access for different user groups: staff, students, parents.
Information: Student name, year level, teacher name and email
Access: usually principal, AP, admin staff, teachers (create not publish), (view only) parents and students
RDA suggestions: Operational correspondence (7 years)

Events Management

Manages all aspects of school events including student excursions, community events. Parents can provide consent for excursions and events
Information: Student name, year level, family contact details including contact flag, family fees and billing information. Higher risk if using health information: allergies, disability, accessibility requirements
Access: usually principal, AP, admin, leadership team, teachers, (limited) parents, (view only) students
RDA suggestions: Camp and excursion records (7 years), Student reference records (1 year after departure)

Health and Wellbeing – Behavioural Management (excluding health information)

For staff to record observations regarding student behaviour and attitude; uniform; confiscation; general health and wellbeing information, and career. Excludes health information.
Information: Student name, DOB, year level, CASES21, family contact details including contact flag, student behavioural management including personalised plan, summary of behavioural incidents and reports, warning notices, behaviour contract, suspension/expulsion, disciplinary action, Staff name, email and class. Higher risk if using health information: allergies, disability, accessibility requirements
Access: principal, AP, leadership team, student welfare coordinators, individual teachers, should be restricted to "need to know" only.
RDA suggestions: expulsion, suspension and welfare records (1 year* after departure), incident records (7 years, where incident is not reported to Emergency and Security Management or the Victorian Workcover Authority directly or via CASES)
*Health and welfare type records may be amended to minimum 25 years after DOB by new Schools RDA (currently in progress)

Health and Wellbeing – Support for special needs or at risk students

Record student health and wellbeing for risk management of vulnerable student behaviour or medical needs. This is distinct from records made by SSS workers (which should be kept in SOCS).
Information: Student name, DOB, year level, CASES21, disability assessment, health/social risk information, student disengagement. No information such as criminal records should be stored.
Student support details including: health and wellbeing assessments, medical and accessibility support, appointments, mental health promotion, support referrals, allergy, immunisation, Sick bay/First Aid, out of home care support, Pastoral Care support, homelessness support, daily violence information, student support group, Crisis or disaster support, Resolution meeting, student behavioural management including personalised plan, summary of behavioural

incidents and reports, warning notices, behaviour contract, suspension/expulsion, disciplinary action; Staff name, email and class; family contact details.
Access: principal, AP, leadership team, student welfare coordinators, individual teachers - should be restricted to "need to know" only.
RDA suggestions: see Health and Wellbeing – Behavioural Management

Timetabling

Timetabling system which organises students' classes, Teachers' classes, the rooms or spaces. Possibly could also organise students with mobility issues.
Information: Student name, year level, student education plan, accessibility notes, teacher name
Access: usually principal, AP, admin, leadership team, teachers
RDA suggestions: teacher work books (after admin use). Require ICT supplier to delete information at school's direction.

School Management

Device Management Software

Used to manage school or BYO portable devices, or use of school network facilities by portable devices. May include remote viewing, remote access and location tracking functionality. Can be used by teachers to Software for a teacher to remotely control or monitor linked devices, for example being able to switch monitors on or off, display a single screen or view individual monitors.
Information: Student Name, Year Level, Teacher names, Student or teacher information stored or accessible on the portable device
Access: usually principal, admin, AP, leadership team, school technician, teachers, parents, students
RDA suggestions: destroyed after admin use concluded. Require ICT supplier to delete information at school's direction.

Employee/Staff Timecard

An application to maintain and verify employee hours. Provides reporting and may integrate or provide reporting to inform accounting payroll systems but not hold this information.
Information: Teacher name, timecard information. **Consider carefully if using staff photos and biometrics**
Access: usually principal, AP, business manager, admin, individual teachers
RDA suggestions: Should be in Edupay. Require ICT supplier to delete information at school's direction.

Finance Management - Budgets and Reporting

System to plan, authorise, adjust and forecast budgets. Also includes financial and regulatory evaluation and reporting, compliance attestation, and council reporting.
Information: Staff name and email address. Student information should not be included.
Access: usually principal, AP, business manager, school council, admin, leadership team
RDA suggestions: Business plans and annual financial reports (permanent), periodic financial reports (7 years)

Finance Management - Accounting

Accounting system including invoicing, cash payments reconciliation and procurement functions.
Information: Student name, year level, family contact details, family fees and billing information, eligibility for financial assistance.
Access: usually principal, AP, admin, leadership team, teachers
RDA suggestions: Receipts, expenditure records, banking records (7 years)

Finance Management – Online Payment Systems

Software to manage fundraising, online fee collection, and online payments.
Information: Student name, year level, family contact details, family fees and billing information,
Access: usually principal, AP, admin, leadership team, teachers, parents,
RDA suggestions: receipts, expenditure records, banking records (7 years)

Library Management System

Manages library resources (excluding purchasing) which may include cataloguing, inventory, search functions and user access to read, share and borrow print and electronic materials. This often links with other school functions such as Education - Lesson Delivery/Activities and Ordering System.
Information: Student name, year level, student borrowing records, email, teacher name and email and other information depending on other functions
Access: usually principal, AP, admin, librarian, teachers, students

Ordering Systems – Canteen, Books, Uniforms

Software which allows for ordering of items for students, families and staff. This can include school lunches for students or staff, student books, library books, student uniforms.

Information: Student name, year level, family contact details, food allergies (for canteen ordering only), student size or measurements, teacher name and email, fee and billing information
Access: usually principal, AP, admin, leadership team, teachers, parents, students
RDA suggestions: Receipts, expenditure records, banking records (7 years)

Online Administration Forms and Surveys

Produces forms which can be used for administrative tasks, for example, internal administrative requests, approvals or ordering. Ensures effective management and administration of the school
Information: Staff name and email. **Consider carefully if using: leave requests, disciplinary reports, performance reports.**
Access: usually principal, AP, admin, leadership team, teachers
RDA suggestions: records documenting management of rosters (7 years)

Print Control Technology

System to manage, track and analyse paper printing between individuals and departments or within schools. Ensures effective resourcing and administration.
Information: Staff name, email, ID; Student name, email
Access: usually principal, AP, admin, leadership team, teachers, students
RDA suggestions: destroyed after admin use concluded. Require ICT supplier to delete information at school's direction.

Appendix C: Department Risk Management Framework

Consequence Criteria: This guide provides indicative terms against which the significance of risk is evaluated.

Descriptor	Educational Outcomes	Wellbeing and Safety	Operational	Finance	Reputation	Strategic
Insignificant	• Educational outcomes can be met with workarounds	• Minor injury requiring no first aid or peer support for stress / trauma event	• Objectives can be met with workarounds	• Small loss that can be absorbed	• Internal impact (no external impact)	• Impact can be managed through normal process
Minor	• Learning outcomes / pathways achieved but below target	• Injury / ill health requiring first aid • Peer support for stress / trauma event	• Objectives met with some resource impact • Compliance incident(s) which are not systematic	• Loss of 'consumable' assets, • < 2% deviation from budget • Minor fraud possible	• Adverse comments local community media • Short term stakeholder dissatisfaction / comment	• Minimal impact on critical DET objectives
Moderate	• Student's overall levels of Literacy and Numeracy static • Partial achievement of targeted learning outcomes • Increasing truancy	• Injury / ill health requiring medical attention • Stress / trauma event requiring professional support	• Objectives cannot be met without significant internal reprioritisation • Regulatory breaches resulting in adverse inspections / reports	• Loss of assets • 2% - 5% deviation from budget • External audit management letter	• External scrutiny e.g. VAGO • Adverse state media comment • Stakeholder relationship impacted	• Significant adjustment to resource allocation and service delivery required to manage impact on corporate priority
Major	• National targeted improvements not achieved • Student dissatisfaction with access to pathways / transitions	• Injury / ill health requiring hospital admission • Stress / trauma event requiring ongoing clinical support	• Objectives can only be met with additional resources • Significant staff shortage impacting service delivery • Serious failure to comply with regulations	• Loss of significant assets • 6% - 15% deviation from budget • External audit qualification on accounts • High end fraud committed	• External investigation • Adverse comments national media • Stakeholder relationship tenuous	• Unable to deliver core program / Government priority
Severe	• Literacy and Numeracy decline • Reduction in access to quality pathways and transitions	• Fatality or permanent disability • Stress / trauma event requiring extensive clinical support for multiple individuals	• Multiple objectives cannot be met • Sustained non-compliance to legislation • Adverse Court Ruling	• Loss of key assets • >15 % deviation from budget • Systemic and high value fraud	• Commission of inquiry • National front page headlines • Stakeholder relationship irretrievably damaged	• Unable to deliver several core programs / Government priorities

Likelihood Criteria: This guide provides the indicative terms against which the probability of a risk event occurrence is evaluated.

Descriptor	Description	Indicative %	Indicative Frequency
Almost Certain	Expected to occur	>95%	Multiple times in the next year
Likely	Probably will occur (no surprise)	66-95%	At least once in the next year
Possible	May occur at some stage	26-65%	Once in the next 3 years
Unlikely	Would be surprising if it occurred	5-25%	Once in the next 5 years
Rare	May never occur	<5%	Once in the next 10 years

DET's Risk Rating Matrix: Used to combine consequence with likelihood to determine the overall level of risk.

Risk Rating Matrix		Consequence				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Medium	High	Extreme	Extreme	Extreme
	Likely	Medium	Medium	High	Extreme	Extreme
	Possible	Low	Medium	Medium	High	Extreme
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	Medium

DET's Acceptability Chart: Used to decide whether the risk is acceptable, based on the rating calculated.

Extreme = Unacceptable (must have Executive oversight)	Immediately consider whether the activity associated with this risk should cease. Any decision to continue exposure to this level of risk should be made at Executive Officer level, be subject to the development of detailed treatments, on-going oversight and high level review.
High = Tolerable (with ongoing management review)	Risk should be reduced by developing treatments. It should be subject to on-going review to ensure controls remain effective, and the benefits balance against the risk. Escalation of this risk to senior levels should occur.
Medium = Tolerable (with frequent risk owner review)	Exposure to the risk may continue, provided it has been appropriately assessed and has been managed to as low as reasonably practicable. It should be subject to frequent review to ensure the risk analysis remains valid and the controls effective. Treatments to reduce the risk can be considered.
Low = Acceptable (with periodic review)	Exposure to this risk is acceptable, but is subject to periodic review to ensure it does not increase and current control effectiveness does not vary.