

Privacy Impact Assessment (PIA) Template

CLASS DOJO - 2020

Name of Project/Software:	Class Dojo https://www.classdojo.com/		
Project Manager/Staff Responsible (eg. ICT/Digital Learning/STEM leader):	Sam Streeter		
School/Department/Area:	Ballarat Primary School – Dana St.	Date:	7/04/2020
Email:	ballarat.ps.dana@edumail.vic.gov.au	Phone:	53321301
Executive Owner/Principal:	Natalie Toohey		

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

A Privacy Impact Assessment (PIA) considers the privacy impacts of any new or amended project (both school-based and central-office) or software (free or purchased) 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 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 1

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

Step 2

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

Step 3

- 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 assessments).
- PIA may need to be updated if **new** privacy risks arise from project or software changes.

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
- new uses for existing software or application
- Other (provide details):

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

- 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 - Behavioural Management (excludes health information)
- Health and Wellbeing – Support for Special Needs or At Risk Students
- Timetabling

School/Central Office 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/:

Class Dojo is a classroom communication application where students can upload and showcase their learning via a digital portfolio.

Features include optional feedback points for behaviours and attendance information. Families can log in and view the digital portfolios of their child:

- In the classroom, teachers use ClassDojo to give students encouragement (or “feedback points”) for showing critical skills or strengths - ones like persistence, critical thinking, teamwork, and leadership.
- Outside the classroom, teachers use ClassDojo to engage families and post work for remote learning. Teachers can instantly message parents with text-based messages, pictures, videos, and stickers, and also add posts to Class Story and School Story - a private feed of moments from the classroom and school that only students, parents, “verified teachers,” and school leaders can see.
- Teachers may also add posts to individual Portfolios - a private portfolio of content that only the student, their teachers, school leaders, and the student’s parents can see.
- (Parents may optionally purchase Premium Features to help encourage their children at home.)

Q3. What improvements will this software deliver and what are its benefits?

The school will use Class Dojo as a third party web based service provider to enhance school communication between the school and parents related to their child's learning and activities.

ClassDojo is a school communication platform that helps teachers encourage students in class and engage parents outside the classroom.

Q4. Does this involve other Department, school or other agency (e.g. VCAA) datasets? (Select all applicable)

Risks: data quality, unauthorised access

Access/import. Details of datasets accessed and if one-off/ongoing access: Teachers type in the individual student names, family names and family contact information. Dojo email invitations will be sent to families inviting them to log in and use the application. Teachers use the ClassDojo Apps or the ClassDojo Platform - if multiple devices are used, they will all sync with each other.

Yes, Other. Details of the kind of interaction and what data sets:

Write-back/synced/exported back to other datasets e.g. Cases21 data. Details:

Q5. Who is involved, their roles, what they will do and what information they can access?

(For Central Office – modify this accordingly)

Risks: collection, use & disclosure, unauthorised access

<input checked="" type="checkbox"/> Students	Account: Users	Activity: Students will access teacher work from the class story. They will respond to individual messages from their teacher and they will upload completed work to their portfolio. Access: can only see their own work and other students' public responses in the class story. They cannot see other students work. Student have their own login to sign in.
<input checked="" type="checkbox"/> Teachers [#]	Account: User and Administrators	Activity: Can view all information, set learning tasks, notify families of new work uploaded and moderate comments Access: Can see all parent and student information for their class
<input checked="" type="checkbox"/> Parents [#].	Account: Users	Activity: Can view their child's portfolio and comment on the portfolio. Parents can message teachers directly in the messages section and it is not viewed by other families. Parents can view and comment on the class story section. Access: Can only see their child's portfolio. Does not have access to other students' portfolio or information
<input checked="" type="checkbox"/> ICT supplier: Class Dojo	Account: ICT Supplier	Activity: Provides remote technical support, holds account information and delivers the Class Dojo platform. Further information on what activities they perform can be found here: https://www.classdojo.com/privacy/#how-does-classdojo-use-the-information-it-collects- Access: has full access to all information as it is stored on their platform.

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.g.s. of primary purposes in School's privacy policy or DET Information Privacy Policy)	Where will it be stored? (if unsure, email the supplier)
Student first and last name, age, gender	Personal	Existing	Enable teachers to identify and give feedback to individual students, required for account creation, and student use.	Data stored on AWS servers in the U.S. and MLab in the U.S.A.; back-ups are in the same locations (AWS/MLab in the U.S.A.); Zendesk in the U.S. for support logs; Some personal information (name, email, phone number, school name) may be stored by SurveyMonkey in the U.S.A. if using filling in surveys for ClassDojo. Please refer to https://www.classdojo.com/en-gb/data/?redirect=true for more information.
Parent contact details (gender, mobile number, email, mobile device ID)	Personal	Existing	Required for account creation. Gender is to select the correct title (e.g. Miss/Ms).	
Language preference for teachers, parents and students	Personal	Existing	Enable use of Class Dojo and for the school to communicate with parents	
School name, address, classroom name,	Personal	Existing	To identify the school community.	
Student feedback points	Personal	New	This feature enables teachers to identify and give feedback to individual students on tasks they share and assist with future learning.	
Photographs, videos, documents, drawings or audio files [confirm what you will use this feature for, and update if photos of students will be included]	Personal	New	Product feature for users to upload and share files of e.g. classwork to share with families. Students and families have been requested by the school to NOT upload any photos/videos of students to the platform. <i>Any video conferencing is done via WebEx.</i>	
Attendance data	Personal	New	Product feature on web and mobile apps to improve the service for teachers/ can view this information	
Geolocation and IP address (parents or teachers)	Personal	New	Used by Class Dojo when parents or teachers are creating an account to search for nearby schools.	As above, plus Algolia and AWS (Elastic Search) in the USA.

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

Feedback Points

- i. ClassDojo can be used to display behaviour reinforcement or goal tracking information about students in the class. These are free text fields where teachers can customise this to display any information.

QR Code Logins

- ii. Students who did not have their own internet capable devices (most) can use their parents' smart phones to log into Dojos and take photos of their homework/projects, etc. to upload to their Dojo accounts. This allowed parents to log in, see all of the students work and comment.

Comment Function

- iii. Parents can log in to view and comment on their child's work. This function can be moderated by the teacher or designated school administrator.

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.

Collection (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 to use ClassDojo.
- 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?

- 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.
- Some. **Ⓛ Address risk in Action Plan (if applicable): inadequate notice**
Details of how and when you provide the required details: insert text
- Yes. Our parent community will be made aware of the use of Class Dojo at enrolment, website, information sessions and in the newsletter
 - Annual Collection notice is provided to parent Term 1
 - Advice/information included in Newsletter each term
 - Access information provided and parent/teacher conferences
 - School's Digital Learning Statement which states what ICT systems the school uses and alternative options made available on schools website
 - The Schools Privacy Policy is linked to our website for viewing.

Q10 If you are collecting new health or sensitive information (see Q6), have you considered if consent is required for the collection of new information?

Valid consent must be: voluntary, informed, specific and current.

- Not Applicable.
- Consent is required.

Reason:

When the school collected this information at enrolment, families were informed that the school uses online tools for a variety of purposes, including education and communication purposes. We use an opt out option which is clear in all communication regarding Dojo. The school will notify relevant families and provide the option to families for their child to opt-out of using this application. Photography – Student photos will not be used on the platform and families will be encourage to not upload any photos of their child.

- Consent is not required.

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 information to Class Dojo is consistent with the primary purpose of collection. The school will notify all involved families and provide the option to families for their child to opt-out of using this application.

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. Explain why there is a reasonable expectation: The use and disclosure of information to Class Dojo is consistent with the primary purpose of collection See questions 10, 11. Also, ClassDojo have stated that they will not market to students: <https://www.classdojo.com/privacy/#how-does-classdojo-use-the-information-it-collects->

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 or other measures in place. Details:
 - Teachers are able to see the information for their year level only. Teachers can also moderate comments and approve or decline comments from being shared.
 - Parents and families can only view and comment on their child's portfolio only.
 - Students can only view their own portfolios and tasks/comments on class story
 - Student, parents and teachers have a login and password to access their dojo account.

Q14 Based on your response in Q6, if you are using unique identifiers, are you using unique identifiers only when permitted?

- Not applicable, not using those unique identifiers (e.g. VSN, CASES21 ID).
- No. **ⓘ Address risk in Action Plan:** *unpermitted use of unique identifiers*
- Yes. Details of why it is permitted:

Q15 Based on your response in Q6 about whether the information is stored or access 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*
- Yes. Details of steps taken:
 - a) The Class Dojo website <https://www.classdojo.com/en-gb/privacy/?redirect=true#how-does-classdojo-protect-and-secure-my-information-> provides this information, representing that they will apply similar protections:

ClassDojo has been certified by iKeepSafe, an FTC-approved COPPA Safe Harbor, for compliance with their COPPA Safe Harbor program. We use security industry best practices to protect personal information, including using encryption and other security safeguards to protect personal information, detailed here.
 - c) The school will also notify families and provide the opportunity to opt out of their child using the application.

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: If requested, students could be given an alias to use when accessing Class Dojo. Although this may work for individual students, it would not be efficient to use this method for multiple students. Student have an avatar to identify themselves.

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:

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. Details of existing process: Classroom teachers will be required to review and update classroom lists on a regular basis (when student enrolments change and/or at the end of each term. If a student leaves, their account will remain open for 14 days to allow for the student to retrieve personal information.

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 central office projects)

No. **Ⓢ Address risks in Action Plan:**

- *unsecured portable devices*
- *access not revoked promptly when no longer required*
- *access by unauthorised staff or 3rd parties*
- *misuse due to lack of training*
- *staff/students unaware of acceptable use*
- *information unencrypted*
- *no access/audit logs*

Yes. Password controls will be implemented to comply with DET password policy:

- *access reviewed and revoked promptly when no longer required*
- *access restricted to authorised staff*
- *ongoing staff training*
- *staff/students/parents all aware of acceptable use*
- *information encrypted*
- *access/audit logs maintained for set periods*
- *no generic log-ins.*

Q20 Does your activity have processes that comply with the DET's data retention and disposal requirements ([Schools](#) and [Central Office](#))?

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. Details of steps taken: Removal of student records and portfolios after departure from the school.

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 <i>* Suggestions are not exhaustive; amend/add/delete to ensure risks are relevant for your school or project</i>	Risk Rating <i>* based on existing controls in Part 1</i>	Action Required <i>* Some suggested actions below, not all are relevant. Amend as needed. Suggestions are not exhaustive.</i>	Responsible Person/Area	Timeframes
1. More information is collected, used or disclosed that is necessary (Q5/Q6/Q7/Q8/Q13/Q14)	Consequence: Minor Likelihood: Unlikely Risk Rating: Low	<ol style="list-style-type: none"> 1. Review table in Q6 and reduce personal information e.g. to first name or first name + initial only 2. No use of student photos as avatars 3. Remove use of other unique identifiers 	Assistant Principal	Annual
2. Consent for collection or use/disclosure of information is not obtained when required or invalid consent (Q7/Q10/Q11/Q12/ Q14/ Q15)	Consequence: Moderate Likelihood: Possible Risk Rating: Low	Opt-out consent is sufficient as it relates to a standard school function For current term 2 remote learning, parents have been informed in the Continuity of Learning handbook for families (page 9)	Principal and Assistant Principal	Start of the year and upon enrolment
3. Unexpected use: ICT supplier uses information for marketing or other purposes without consent or de-identification (Q5/Q7/Q12/Q13)	Consequence: Minor Likelihood: Unlikely Risk Rating: Low	Use DET template contract with ICT supplier or ensure Terms & Conditions include model terms	Principal and Assistant Principal	As required
4. Unauthorised access: Staff changing roles that no longer require them to access the information (Q13/Q18/ Q19)	Consequence: Major Likelihood: Possible Risk Rating: Medium	Regular review of users (6 monthly and when advised of role changes)	Teachers, Principal and Assistant Principal	As required
5. Data will be accessed and/or transferred outside Victoria without similar protections (Q6/ Q15)	Consequence: Moderate Likelihood: Rare Risk Rating: Low	<ol style="list-style-type: none"> 1. Use DET template contract or ensure T&Cs include model terms 2. Data to be stored onsite and service provider has no access 3. 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. 	Principal and Assistant Principal	Annual

6.	Inadequate process to ensure information is kept up to date (Q5/Q18)	Consequence: Moderate Likelihood: Unlikely Risk Rating: Low	If any staff wants to update sensitive information then there is 2 step process where it has to be checked off by another staff.	Principal and Assistant Principal	Annually
7.	Misuse and unauthorised disclosure of information by staff (Q19)	Consequence: Minor Likelihood: Rare Risk Rating: Low	<ol style="list-style-type: none"> Staff to be trained and provided with guidelines regarding Schools Privacy Policy. Staff to be trained in how to upload material and use the software Create access protocol which includes managing access requests and a Register of access requests and changes Communication plan and staff training to be developed to minimise risks of misuse and maximise benefits 	Principal and Assistant Principal	As required
8.	Misuse and unauthorised access by students and parents (Q5/Q7/Q19)	Consequence: Minor Likelihood: Possible Risk Rating: Medium	<ol style="list-style-type: none"> 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, photos and videos of students, other student's information, health information, sensitive information, bank details, home address etc (delete what is not applicable) Ensure all communications are moderated Establish a process to regularly monitor all information posted and uploaded 	Principal and Assistant Principal	As required
9.	Unauthorised access by ICT supplier or unauthorised third party (Q5/Q7/Q19)	Consequence: Insignificant Likelihood: Rare Risk Rating: Low	<ol style="list-style-type: none"> Set out clear procedure with ICT supplier regarding remote access and remote tech support Use DET contract templates and put in writing agreed process with ICT supplier on their level of access 	School Technician, Principal and Assistant Principal	As required
10.	Unauthorised access through portable devices (Q7/Q19)	Consequence: Moderate Likelihood: Possible Risk Rating: Medium	<ol style="list-style-type: none"> Ensure compliance with <u>DET Portable Storage Device Security Policy</u> Ensure staff and TSSP are aware of DET Portable Storage Device Policy – raised during staff meeting/ email reminder from principal Password protection in portable devices 	Principal and Assistant Principal	As required
11.	Unauthorised access of accounts due to insecure passwords (Q7/Q19)	Consequence: Minor Likelihood: Possible Risk Rating: Medium	<ol style="list-style-type: none"> All staff, students and authorised users are notified of <u>DEI password policy</u> principles Ensure that password controls are implemented that comply with the <u>DET password policy</u> No generic log ins are used Two-factor authentication Encryption of passwords 	eLearning/ICT coordinator School Technician	As required

12.	Information kept longer than required (Q5/Q20)	<p>Consequence: Minor Likelihood: Rare Risk Rating: LOW</p>	<ol style="list-style-type: none"> 1. Contact DET Records Management regarding appropriate RDA guidance on records created through the project/activity 2. Ensure ICT supplier contracts include clauses which complies with IPPs (see draft sample clauses) or use DET contract template 3. If ICT supplier is providing storage, identify for how long, who is responsible, and security expectations when there are data exports 	Teacher and school technician	Before implementation
-----	--	---	--	-------------------------------	-----------------------

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:	Sam Streeter	Title:	Assistant Principal
Signature:		Date:	11.4.2020

Executive Business Owner/Principal (Sponsor) Endorsement

I acknowledge and accept the risks and associated actions required as outlined in this document.

Name:	Natalie Toohey	Title:	Principal
Signature:		Date:	11/4/2020

*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:	28 May 2020

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.

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](#)
- [Central office](#) and [schools](#): ICT Acceptable Use Policy
- Department: [Portable Storage Devices Security Policy](#) (for staff personal devices)

Procurement

- [Central office](#) 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 central office: 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 [Central Office](#)

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	<ul style="list-style-type: none"> Educational outcomes can be met with workarounds 	<ul style="list-style-type: none"> Minor injury requiring no first aid or peer support for stress/trauma event 	<ul style="list-style-type: none"> Objectives can be met with workarounds 	<ul style="list-style-type: none"> Small loss that can be absorbed 	<ul style="list-style-type: none"> Internal impact (no external impact) 	<ul style="list-style-type: none"> Impact can be managed through normal process
Minor	<ul style="list-style-type: none"> Learning outcomes / pathways achieved but below target 	<ul style="list-style-type: none"> Injury / ill health requiring first aid Peer support for stress / trauma event 	<ul style="list-style-type: none"> Objectives met with some resource impact Compliance incident(s) which are not systematic 	<ul style="list-style-type: none"> Loss of 'consumable' assets, < 2% deviation from budget Minor fraud possible 	<ul style="list-style-type: none"> Adverse comments local community media Short term stakeholder dissatisfaction / comment 	<ul style="list-style-type: none"> Minimal impact on critical DET objectives
Moderate	<ul style="list-style-type: none"> Student's overall levels of Literacy and Numeracy static Partial achievement of targeted learning outcomes Increasing truancy 	<ul style="list-style-type: none"> Injury / ill health requiring medical attention Stress / trauma event requiring professional support 	<ul style="list-style-type: none"> Objectives cannot be met without significant internal reprioritisation Regulatory breaches resulting in adverse inspections / reports 	<ul style="list-style-type: none"> Loss of assets 2% - 5% deviation from budget External audit management letter 	<ul style="list-style-type: none"> External scrutiny e.g. VAGO Adverse state media comment Stakeholder relationship impacted 	<ul style="list-style-type: none"> Significant adjustment to resource allocation and service delivery required to manage impact on corporate priority
Major	<ul style="list-style-type: none"> National targeted improvements not achieved Student dissatisfaction with access to pathways / transitions 	<ul style="list-style-type: none"> Injury / ill health requiring hospital admission Stress / trauma event requiring ongoing clinical support 	<ul style="list-style-type: none"> Objectives can only be met with additional resources Significant staff shortage impacting service delivery Serious failure to comply with regulations 	<ul style="list-style-type: none"> Loss of significant assets 6% - 15% deviation from budget External audit qualification on accounts High end fraud committed 	<ul style="list-style-type: none"> External investigation Adverse comments national media Stakeholder relationship tenuous 	<ul style="list-style-type: none"> Unable to deliver core program / Government priority
Severe	<ul style="list-style-type: none"> Literacy and Numeracy decline Reduction in access to quality pathways and transitions 	<ul style="list-style-type: none"> Fatality or permanent disability Stress / trauma event requiring extensive clinical support for multiple individuals 	<ul style="list-style-type: none"> Multiple objectives cannot be met Sustained non-compliance to legislation Adverse Court Ruling 	<ul style="list-style-type: none"> Loss of key assets >15% deviation from budget Systemic and high value fraud 	<ul style="list-style-type: none"> Commission of inquiry National front page headlines Stakeholder relationship irretrievably damaged 	<ul style="list-style-type: none"> 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.

Likelihood	Consequence		
	Insignificant	Minor	Major
Almost Certain	Medium	High	Extreme
Likely	Medium	Medium	Extreme
Possible	Low	Medium	High
Unlikely	Low	Low	Medium
Rare	Low	Low	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 reviews)	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 reviews)	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.