Privacy Impact Assessment

Name of Project/Software:	**Seesaw**		
Project Manager/Staff Responsible *(eg. ICT/Digital Learning/STEM leader)*:	**Michael Uzunovski**		
School/Department/Area:	**Albanvale Primary School**	Date:	**21/04/2020**
Email:	**Albanvale.ps@edumail.vic.gov.au**		
Executive Owner/Principal:	**Susanna Vermezovic**		

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 ⓘ 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
☐ 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
☐ 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 central office projects. Some are **specific** to schools or central office 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 - 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/activities, please **also** specify: Allows the school, students and parents to share photos and classwork.

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

Currently:

We were using physical goal setting portfolios that move up with the students as they progress through the year levels. Throughout the year. At Learner conferences, the students sit with their parents and discuss their learning using the portfolio as stimulus. At the conclusion of the year, the students take all of their work out of the portfolio and it gets passed onto the next teacher.

Benefits:

- The parents will have constant access to **their own child's portfolio.**
- Parents will be able to record feedback on **their own child's portfolio or any document shared by the teacher.**

- Ease of access for the students as they will be able to log into **their own portfolio** from any location with any compatible device. This will support home learning.
- Reduction of paper
- Enhanced communication with parents students and teachers mean that teachers can efficiently act on feedback to better support students learning
- Supports our continuous Goal Setting and reporting process

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. Details of datasets accessed and if one-off/ongoing access: Teacher or administrator to upload student and parent details extracted from eCASES (***Note** - please confirm, may only be applicable for paid version).
☐ Write-back/synced/exported back to other datasets *e.g. Cases21 data*. Details: [insert text].
☐ 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?
ⓘ **Risks:** *collection, use & disclosure, unauthorised access*

☒ Students [# e.g. 300]	Account: User	Activity: Can log-in to participate in class activities, view work, retrieve homework, submit their own journal work and view and comment on other students' work. Access: Can see their information (including feedback and assessment provided by teachers), the information of other students and their parents' responses to approved assessment. Cannot submit content without teacher approval.
☒ Staff:	Account: Admin/User	Activity: Can create student accounts, manage grade settings, approve submitted assessments, submit journal work for completion by students, provide feedback to students in relation to their work and consider parent comments. Access: Can see all student and parent information.
☒ Parents	Account: User	Activity: Can view and comment on their child's classwork, photos and/or journal work. Access: Can only see and post comments on their child's journal, cannot see or comment on other students' journals.
☒ ICT supplier: Seesaw	Account: Admin	Activity: Can provide remote support. Access: Has full access to all student information as it is stored in its cloud service but only for permitted purposes.
☒ Leadership team, administration staff and school technician	Account: Admin	Activity: Provide support, roll over and set up Access: Has full access to all student information as it is stored in its cloud service but only for permitted purposes

Q6. Fill out this information table (See **Appendix B** for typical information for common school functions/activities)

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 & initial of surname of student	*Personal*	*Existing*	*Enables teachers to identify and give feedback to individual students and parents.*	*Hosted in Amazon Web Services cloud in the USA. See https://help.seesaw.me/hc/en-us/articles/204472519-Where-is-my-data-stored-*
Student form group	*Personal*	*Existing*	*Enables students, teachers and parents to identify the classroom which they are accessing and are grouped under.*	
Photos/videos of student doing activities	*Personal*	*New*	*Enables school to communicate with parents about student learning activities.*	
Student and parent email addresses and passwords	*Personal*	*Existing*	*Enables teachers to identify, contact and give feedback to individual students and parents.*	
Journal content including any non-student photos, drawings, files, notes, hyperlinks and any other documented student learning	*Personal*	*New*	*Enables students, parents and teachers to communicate about student learning activities.*	
Comments on journal content including written comments and oral voice recordings uploaded to the system	*Personal*	*New*	*Enables students, parents and teachers to communicate about student learning activities.*	
Messages sent and received via Seesaw by teachers, parents and students	*Personal*	*New*	*Enables students, parents and teachers to communicate about student learning activities.*	
The school's details	*n/a*	*Existing*	*Enables Seesaw to identify the school.*	
Information regarding	*Personal*	*New*	*Enables Seesaw to investigate, prevent and detect activities*	

internet usage including webpages visited and search terms			*that may violate the law or applicable regulations and to ensure accounts comply with school policies.*	

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: [insert text].

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. ☐ Yes. ⓘ **Address risk in Action Plan:** *unnecessary information collected or used* (***Note** - consider if you have added items in Q6)
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;* *d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind;* *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* ☐ Not applicable. No notice is required because no new information collected or indirect collection and notification would result in serious threat to life/health. ☒ Yes. Details of how and when you provide the required details. We recommend attaching copies of the proposed collection notices: [insert text]. *At the beginning of each school year, students unpack the school Digital Technologies Responsible Use Agreement which includes sharing information and Safe use of the Seesaw Platform. Parents are informed the associated data collection and privacy practices in place and are asked the sign the agreement if they comply and accept. These agreements are collated and stored in school records.* ☐ 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: (***Note** - if using student photos, parental consent is required as part of the DET's policy) Our school will use Seesaw to take and upload photographs of students. We will: • seek consent from families to use student photographs in Seesaw; and • have a process in place to ensure that the student of any of the families who opt out will not have their photo uploaded. *E.g. collecting sensitive or health information and no other exception applies* ☒ Consent is not required: No new sensitive or health information collected. However, because it is appropriate here for the school to provide parents with the choice as to the kind of education technology in the classroom, the school will take additional steps to offer the families alternative arrangements in the notification.
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?	☐ No. ⓘ **Address risk in Action Plan:** *inadequate notice for secondary use* ☒ Yes. The use and disclosure of information when using Seesaw is for educating students and communicating with parents (primary purpose) and disclosure to Seesaw as the school's contracted cloud service provider, as part of the activity, is a related secondary purpose. Seesaw does not sell the information or advertise to students.
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*	☐ No. ⓘ **Address risk in Action Plan:** *unexpected use/disclosure* ☒ Yes. Explain why there is a reasonable expectation: When the school collected this information at enrolment, families were informed that the school uses online tools for a variety of purposes, including educating students and communicating with parents. The school also links to the school's privacy policy.
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: Access is limited by the role of the individual accessing it (i.e. student, teacher, or parent) and access is granted on an individually approved basis by the teachers and administrators (if applicable) for this service.
Q14 Based on your response in Q6, if you are using unique identifiers, are you using them only when permitted?	☒ Not applicable, not using unique identifiers. ☐ No. ⓘ **Address risk in Action Plan:** *unpermitted use of unique identifiers* ☐ Yes. Details of why it is permitted: If using the unique identifiers for the paid version of Seesaw, used eCASES/CASES ID to ensure continuity and not VSN.

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.*

☐ No. ⓘ **Address risk in Action Plan:** *unprotected transborder data flow*
☒ Some. Details of steps taken: Please see https://web.seesaw.me/privacy and https://web.seesaw.me/privacy-policy.

Seesaw's privacy promises and privacy policy states that:

- **We never sell your data or student data:** We will never sell or rent your data or create profiles of Seesaw users to sell. Our business model is straightforward: we charge schools and districts for optional, additional features on top of our free product.
- **We never advertise in Seesaw:** We have no interest in advertising in Seesaw. Again, our business model is straightforward: we charge schools and districts for optional, additional features on top of our free product.
- **We don't own the content you add to Seesaw:** Students and their schools own the work added to Seesaw. If you'd ever like to save your content elsewhere or use a different product, you can download what you've added to Seesaw to your computer or mobile device. You can also delete your account at any time and we will permanently delete your account and all associated data within 60 days.
- **Student work is private to the classroom by default:** Teachers control what is shared and with whom. Unless teachers choose to share, no student work is visible outside of the classroom. Teachers can choose to invite family members to see the work their child has added to Seesaw or post some items more publicly (such as to a Seesaw blog).
- **We use the latest security industry best practices to protect you:** This means we do things like provide secure communication with our servers at all times, encrypt journal content at rest, and run regular 3rd party security audits to make sure your information is secure.
- **We are transparent about our practices, and will notify you if things change:** We strive to make our policies easy to understand. If anything substantial were to change with our privacy practices, we would let you know. The privacy policy and terms you agreed to will still apply unless you accept new terms.
- **We are compliant with FERPA, COPPA, and GDPR:** Seesaw is fully compliant with these important laws so it's safe to use Seesaw in the classroom.

Seesaw also states that:

We only use this information to provide our services to users. For example we use this information to:

- Allow users to access and use our service by verifying their identity and storing their Journal Content.
- Provide teachers, schools, and family members with customer support.
- Notify users about activity on and updates to their account or their child's account (if they've indicated in your account settings that you'd like notifications).
- Research, understand, and analyse trends of users to improve and develop new features for our products.
- Promote new Seesaw products and services to teachers, parents and schools.

	• Investigate, prevent, and detect activities on our service that we believe may violate the law or applicable regulations. We may, at the request of a school, investigate accounts to determine whether they comply with school policies.
	
	(https://help.seesaw.me/hc/en-us/articles/360002362152-Who-are-Seesaw-s-subprocessors-) Our sub processors have all signed a Data Protection Agreement with us, which stipulates that any data we share with them will be used exclusively to provide services to us and not for any other purposes.
	
	Currently we use sub processors to:
	
	• Host and deliver Seesaw
	  ○ Amazon Web Services (Data centre management)
	  ○ LaunchDarkly (Beta testing support)
	
	• Communicate with teachers, families, and administrators
	  ○ Autopilot (Sending emails)
	  ○ Boomerang (Sending emails)
	  ○ Mailchimp (Sending emails)
	  ○ Mailgun (Sending emails)
	  ○ Twilio (Sending text messages)
	  ○ Versal (Provide online courses)
	
	• Run our internal operations
	  ○ Zendesk (Software for customer support)
	  ○ Ada (Software for customer support)
	  ○ Shopify (Operating the Seesaw store)
	  ○ Salesforce (Manage customer relationships)
	  ○ Outreach (Organize communications with schools)
	  ○ Wufoo (Collect interest in Seesaw for Schools)
	  ○ Docusign (Electronically sign contracts with schools)
	  ○ SaaSOptics (Manage our internal finances)
	  ○ Quickbooks (Manage our internal finances)
	  ○ Survey Monkey (Conduct surveys and user research)
	  ○ Google (Manage emails, calendars, and documents)
	
	Seesaw TOS state:
	
	We don't own the content you provide – students and their schools own all Student Data added to Seesaw.

Q16 Must individuals be identifiable (i.e. not anonymous) during this project or when using this software?	☒ 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.

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: If you are a parent or teacher, you can update the information associated with your Seesaw account directly by logging into your Seesaw account and viewing the account settings tab in your profile. Student information is updated in real time by the teacher (administrator for each grade).
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. Details of existing steps taken to enhance Seesaw security: Students are informed of acceptable use when using digital technologies/school has a policy about acceptable use of digital technologies. All comments and posts are approved by the teacher or the administrator before they appear in the student's journal. Access is granted to students via a QR code generated by the classroom teacher after they have created the student account. (

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.

Requests to delete all account information and content uploaded on Seesaw are to be sent via email to help@seesaw.me. Seesaw will then delete data within 60 days as per the retention policy located in the privacy centre, please see https://web.seesaw.me/privacy. In addition, students' work portfolios and the school's communication with parents regarding their work portfolios are part of student records and these will be subject to the General Retention and Disposal Authority for School Records and will have to be retained for a minimum period of 4 months before disposal. See Action Plan.

See *Appendix B* for further information

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

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.

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.

RDA suggestions: Student reference records (1 year after departure), Operational correspondence (7 years)

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 (i.e. the development of consent forms, security access protocols, system integrity improvements etc). 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 disclosed on Seesaw than is necessary for the purposes. Inappropriate use of information by staff: e.g. unnecessary personal information or highly delicate information or health information might be accidentally uploaded (Q5/Q6/Q7/Q8/Q13/Q14)	Consequence: Moderate Likelihood: Unlikely Risk Rating: Medium	1. Create policy/operational protocol for what info can be shared on Seesaw and acceptable uses including: o What should and should not be uploaded on student and class journal o Will class journal be used? If so, what should not be uploaded on class journal o Who can access student journal and class journal o Permitted sharing of class content and disable sharing outside school community (i.e. FB and twitter) 2. Share protocol with staff to maximise benefits of use and minimise risks of misuse. Principal or Leading Teacher to raise this during staff meeting and/or send email before implementation, and share with all new staff at induction.	Curriculum Leading Teacher	Before implementation & ongoing
2.	Lack of notification to parents about how the information is collected, used or disclosed (Q7/ Q9/Q11)	Consequence: Moderate Likelihood: Unlikely Risk Rating: Medium	1. Link DET Schools Privacy Policy. 2. Notification to parents about Seesaw by updating Digital Learning Statement/specific. collection notice/school newsletter (any one or more combination). Notification states parents to contact school if they wish to discuss alternative arrangements. 3. Check school processes to ensure DET standard enrolment and primary/secondary annual collection statements are used. 4. Review school's video and photo policy.	Curriculum Leading Teacher/Principal Privacy Officer can review notification	Before implementation
3.	Consent for collection or use/disclosure of information is not obtained when required or invalid consent	Consequence: Moderate Likelihood: Possible Risk Rating: Medium	Update photo permission form or include consent for use of photos in the notification.	Curriculum Leading Teacher Privacy Officer can assist	Before implementation

	(Q7/Q10/Q11/Q12/ Q14/ Q15)				
4.	Unauthorised access: Staff changing roles or departing students that no longer require them to access the information (Q13/Q18/ Q19)	Consequence: Minor Likelihood: Possible Risk Rating: Low	Add to protocol: handover and account deletion/transfer/password reset for exiting staff or students. Regular review of users (annually by office administrator staff) .	Curriculum Leading Teacher	Before implementation & ongoing
5.	Data will be accessed and/or transferred outside Victoria without similar protections (Q6/ Q15)	Consequence: Minor Likelihood: Unlikely Risk Rating: Low	School is using the paid version and will be using the DET template contract	Curriculum Leading Teacher/Principal	Before implementation
6.	Misuse and unauthorised access by students and parents (Q5/Q7/Q19) [e.g. parent make abusive or inappropriate comments]	Consequence: Moderate Likelihood: Unlikely Risk Rating: Low	1. Include in notification to parents (and share with students): o expectations of acceptable use o what information should not be posted/ uploaded: e.g. personal mobile or phone numbers, personal photographs and videos unrelated to school work, other student's information, health information, sensitive information, bank details, home address etc o parents to supervise at home 2. Include in protocol: o ensure all communications are moderated and approved by the teacher o establish a process to regularly monitor all information posted and uploaded 3. Turn off functions that create unacceptable risk including teachers to approve all comments. 4. Explicit teaching of safe use and practices on Seesaw as part of the ICT learning program	Curriculum Leading Teacher	Before implementation & ongoing
7.	Unauthorised access by ICT supplier or unauthorised third party (Q5/Q7/Q19)	Consequence: Minor Likelihood: Unlikely Risk Rating: Medium	1. Include in notification to parents and students: o educate students on cyber safety and remind students about logging out o ensure parents are aware that they should not access Seesaw using their child's login details and should only use their own QR code o parental notification reminders that QR codes must be kept safe 2. Use DET contract templates (if possible)	Curriculum Leading Teacher/Principal	Before implementation

8.	Unauthorised access through portable devices or insecure passwords (Q7/Q19) (e.g. it might be when teachers log in on personal devices or parents or students log in to their portable devices which gives people access to information they shouldn't have)	Consequence: Minor Likelihood: Possible Risk Rating: Low	1. Ensure compliance with DET Portable Storage Device Security Policy (https://edugate.eduweb.vic.gov.au/Services/IT/ServiceDocuments/Password%20Policy.pdf) 2. Ensure staff and TSSP are aware of DET Portable Storage Device Policy – raised during staff meeting/ email reminder from principal 3. Password protection for portable devices 4. share this link about setting strong passwords, and changing passwords regularly (at least annually) 5. Add to protocol – change passwords every term	Curriculum Leading Teacher/Principal	Before implementation
9.	Information kept longer than required (Q5/Q20)	Consequence: Minor Likelihood: Unlikely Risk Rating: Low	Add to protocol: 1. Have a process for retention and deletion of student records for 1 year after departure. (***Note** - students' work portfolios and the school's communication with parents regarding their work portfolios are part of student records and these will be subject to the General Retention and Disposal Authority for School Records and will have to be retained for a minimum period of 4 months before disposal.) 2. 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	1.Project Manager/ Responsible Staff 2. Project manager/DET legal to review	Before implementation
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 2. (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

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:	Michael Uzunovski	Title:	Assistant Principal
Signature:		Date:	21/04/2020

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

Name:	Susanna Vermezovic	Title:	Principal
Signature:		Date:	21/04/2020

*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:	

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	• 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.