POLICY STATEMENT:

This policy outlines Ballarat Grammar's policy on its uses and management of personal information. The School is bound by the Australian Privacy Principles contained in the *Privacy Act* 1988(Cth) and will annually review this Privacy Policy to take account new laws and the changing school environment.

DEFINITIONS:

Sensitive Information- means information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences or criminal record, that is also personal information; and health information about an individual.

Personal Information- means information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not. (s6 *Privacy Act* 1988(Cth))

Health Information- means information relating to medical records, disabilities, immunisation details, individual health care plans, counselling reports, nutrition and dietary requirements.

Serious Harm- could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the school's position would identify as a possible outcome of the data breach. The Explanatory Memorandum also emphasises that though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not in itself be sufficient to require notification unless a reasonable person in the school's position would consider that the likely consequences for those individuals would constitute serious harm.

DETAIL:

Part 1- Type of Information

1. Ballarat Grammar collects and holds personal, sensitive and health information regarding:
   1.1 Students and parents and/or guardians ('Parents') before, during and after the course of a student's enrolment at the School;
   1.2 Job applicants, staff members, volunteers and contractors; and
   1.3 Other people who come into contact with the School.
2. This information is collected by the following means:
   2.1 Parents, students or members of the school community completing forms, attending face to face meetings, interviews and telephone calls.
   2.2 In some circumstances the School may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school.
3. In some cases where the School requests personal information about a student or Parent, if the information requested is not obtained, the School may not be able to enrol or continue the enrolment of the student.

Please note: Under the Privacy Act 1988(Cth) the Australian Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and an employee.

Part 2- Use of Information

1. The School will use personal, sensitive and health information it collects from you for the primary purpose of collection, and for other related secondary purposes which might reasonably be expected, or to which you have consented.
2. The purpose in which the School may collect personal, sensitive and/or health information include but are not limited to:
   - 2.1. Enabling the School to provide ongoing education and pastoral care for students
   - 2.2. Fulfilling our legal obligations regarding our duty of care and child protection obligations;
   - 2.3. Keeping Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
   - 2.4. Day-to-day administration;
   - 2.5. Marketing, promotional and fundraising activities;
   - 2.6. Supporting the activities of school associations such as Old Grammarians;
   - 2.7. Supporting community-based causes and activities in connection with the School's functions or activities;
   - 2.8. Assisting the School improve its daily operations;
   - 2.9. School administration including insurance purposes;
   - 2.10. Looking after students' educational, social and medical well-being; and
   - 2.11. Seeking donations and marketing for the School.
3. The School may collect personal information regarding job applicants, staff members and contractor for the primary purpose of assessing and (if successful) to engage the applicant, staff member or contractor, as the case may be. This personal information may be used for the following purposes:
   - 3.1. In administering the individual's employment or contract, as the case may be;
   - 3.2. For insurance purposes;
   - 3.3. Seeking funds and marketing for the School;
   - 3.4. To satisfy the School's legal obligations, for example, in relation to child protection legislation.
4. The School may also collect personal information regarding direct or indirect volunteers who assist the School in its functions or conduct associated activities, to enable the School and the volunteers to work together and maintain its commitment to a child safe environment.

Part 3- Disclosure of Personal Information

1. The School may disclose personal information, including sensitive information, held about an individual to:
   - 1.1 Another school;
   - 1.2 Government departments;
   - 1.3 Medical practitioners;
   - 1.4 People providing services to the School, including specialist visiting teachers and sports coaches;
   - 1.5 Recipients of School publications, like newsletters and magazines;
   - 1.6 Parents; and
   - 1.7 Anyone to whom you authorise the School to disclose information.

Part 4- Privacy in Education Settings

1. Early childhood services are obligated by law, service agreements, and licensing requirements to comply with the privacy and health records legislation when collecting personal and health information about individuals.
2. The Health Records Act 2001 (Part 1, 7.1) and the Privacy and Data Protection Act 2014 (Vic) (Part 1, 6 (1)) include a clause that overrides the requirements of these Acts if they conflict with other Acts or Regulations already in place. For example, if there is a requirement under the Education and Care Services National Law Act 2010 or the Education and Care Services National Regulations 2011 that is inconsistent with the requirements of the privacy legislation, services are required to abide by the Education and Care Services National Law Act 2010 and the Education and Care Services National Regulations 2011.
3. In line with the Victorian Government's Roadmap for Reform, Education State reforms and broader child safety initiatives, Part 6A of the Child Wellbeing and Safety Act 2005 (the Act) was proclaimed in

September 2018. The Act established the Child Information Sharing (CIS) Scheme, which enables sharing of confidential information between prescribed entities in a timely and effective manner in order to promote the wellbeing and safety of children. The Act also authorised the development of a web-based platform that will display factual information about children's participation in services known as the Child Link Register (to become operational by December 2021). The Child Link Register aims to improve child wellbeing and safety outcomes, monitor and support the participation in government-funded programs and services for children in Victoria.

4. Alongside the CIS Scheme, the Family Violence Protection Act 2008 includes the Family Violence Information Sharing (FVIS) Scheme and the Family Violence Multi-Agency Risk Assessment and Management (MARAM) Framework, which enables information to be shared between prescribed entities to assess and manage family violence risk to children and adults. The MARAM Framework can be used by all services including ECEC services that come into contact with individuals and families experiencing family violence. The MARAM Framework aims to establish a system-wide shared understanding of family violence. It guides professionals across the continuum of service responses, across the range of presentations and spectrum of risk. It provides information and resources that professionals need to keep victim survivors safe, and to keep perpetrators in view and hold them accountable for their actions.

Part 5- Sensitive Information

1. Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Part 6- Management and security of personal information

1. The School's staff are required to respect the confidentiality of students' and Parents' personal information and the privacy of individuals.
2. The School has in place steps to protect the personal information the School holds from misuse, loss, unauthorised access, modification or disclosure, by various methods including locked storage of paper records, campus security and password access to computerised records.
3. If you would like further information about the way the School manages the personal information it holds, please contact the Headmaster's Personal Assistant.

Part 7- Requesting Personal Information

1. Under the Privacy Act 1988(Cth), an individual has the right to obtain access to personal information which the School holds about them and to advise the School of any perceived inaccuracy. There are some exceptions to this right set out in the Act.
2. Students will generally have access to their personal information through their Parents, but older students may seek access themselves.
3. To make a request to access any information the School holds about you or your child, please contact the Headmaster's Personal Assistant in writing.
4. The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

Part 8- Right of Access

1. Generally, the School will refer matters relating to the personal information of a student to the student's Parents.
2. The School will treat consent given by Parents as consent given on behalf of the student and notice to Parents will act as notice given to the student.
3. Parents may seek access to personal information held by the School about them or their child by contacting the Headmaster's Personal Assistant. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable

impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student.

4. The School may, at its discretion, on the request of a student grant that student access to information held by the School about them or allow a student to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances so warranted.

Part 9- Privacy Breaches

1. Commencing 22 February 2018, changes to the *Privacy Act* 1988(Cth) make it compulsory for schools to notify specific types of data breaches (Notifiable Data Breaches or NDBs), to individuals affected by the breach, and to the Office of the Australian Information Commissioner (OAIC). A data breach occurs where "personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference."
2. This requirement applies to all non-government schools, unless they have a revenue of less than $3 million and they do not provide a health service.
3. Not all data breaches will be NDBs. A NDB is defined as a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. Serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.
4. Not all instances of unauthorised access or use of personal information will come under the mandatory reporting regime. The Privacy Act refers to an "eligible data breach", while the OAIC uses the term NDB on its website.
5. Under the Act a data breach must be notified where:
   5.1 There is unauthorised access to, or unauthorised disclosure of, personal information; and
   5.2 A reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the personal information relates.
   Or
   5.3 Personal information is lost in circumstances where:
      5.3.1 Unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
      5.3.2 Assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

Examples of a data breach which may meet the definition of an eligible data breach include when: a device containing a member of the school community's personal information is lost or stolen e.g. a laptop; a database containing personal information is hacked; or personal information is mistakenly provided to the wrong person.

Part 10- Notifiable Data Breach Procedure

1. Where an eligible data breach is suspected or believed to have occurred the School:
   1.1 Carries out a risk assessment in the event that an eligible data breach is suspected which involves;
      1.1.1 Assessing whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach. This must be as prompt and efficient as practicable in the circumstances; and
      1.1.2 Taking all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.

   The School may undertake a risk assessment where an individual has made a complaint in relation to the security of personal information and the school suspects that an eligible data breach may have occurred, but further information is required to ensure the criteria of an eligible data breach is met. If the risk assessment reveals that an eligible data breach has occurred, the school then follows the notification requirements under the Act and notifies both the OAIC and if practicable, the individual/s affected.

   1.2 Prepares a statement of prescribed information regarding an eligible data breach that is believed to have occurred;

1.2.1 The statement includes the following:
1.2.1.1 The identity and contact details of the School;
1.2.1.2 A description of the eligible data breach that the School has reasonable grounds to believe has happened;
1.2.1.3 The kind(s) of information concerned; and
1.2.1.4 Recommendations about the steps that individuals should take in response to the eligible data breach that the School has reasonable grounds to believe has happened.
1.2.2 If the School believes that another entity regulated by the Act is involved in the eligible data breach, the Statement must include information about the other entity or entities.
1.3 Submits the statement to the OAIC as soon as practical after the School becomes aware of the eligible data breach; and
1.4 Takes all reasonable steps to contact all affected individuals or those individuals at risk of being affected directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.
1.4.1 The reasonable steps will involve considerations regarding time, effort or cost of notification.
1.4.2 The School will publish a statement on its website.

Part 11- Complaints handling and Australian Privacy Principles (APP) breaches

1. The APPs require the School to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the School's functions or activities that will enable it to deal with enquiries or complaints about its compliance with the APPs.
2. Any complaints received will be dealt with in accordance with the School's *Complaints Handling* Policy.
3. If the complainant does not believe the complaint was adequately dealt with by the School, that person may make a further complaint to the Privacy Commissioner and seek advice regarding any such complaint from the Privacy Hotline on 1300 363 992. Once referred to the Privacy Commissioner the complaint will be dealt with by way of conciliation or by means as deemed appropriate by the Privacy Commissioner.

Part 12- Legal Proceedings

1. Ballarat Grammar recognises that it is an offence to destroy or interfere with any document that is reasonably likely to be required in evidence in a legal proceeding.
2. As 'reasonably likely' is not a defined expression, the School acknowledges that each category needs to be individually assessed.

Part 13- General

1. The School endeavours to ensure that the personal information it holds is accurate, complete and up to date. A person may seek to update their personal information held by the School by contacting the Headmaster's Executive Assistant of the School at any time.
2. The Australian Privacy Principles require the School not to store personal information longer than necessary.
3. Any complaints in relation to the School's privacy management will be handled as per the School's Complaints Policy.
4. In relation to consent and young people the School follows the guidance from the Association of Independent Schools, as outlined in Annexure A.

Annexure A

Consent and Young People
(specific guidance from the Association of Independent Schools)

The Privacy Act does not distinguish between adults and children and thus clearly envisages that young people are to be afforded rights in respect of their privacy. However, the APPs do not differentiate between children of different ages and thus it is difficult to determine when it is appropriate to seek consent from students.

In relation to consent and young people, the APP Guidelines provide as follows:

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

The Australian Law Reform Commission (ALRC) also considered the issue of consents by children and young people and recommended that the Privacy Act should be amended to provide that where an assessment of capacity to provide consent 'is not reasonable or practicable' an individual of the age of 15 or over should be capable of giving consent and a person under that age should be presumed not to be capable of giving consent.

The ALRC also noted that people with parental responsibility had some authority to make decisions on behalf of their children who lacked capacity if it was part of a duty to provide for their welfare but did not suggest that such authority extended to all situations.

In approaching the issue of privacy for Schools it is important to remember that the underlying arrangement between the School and parents is contractual. Parents are engaging the School to provide schooling for their child on the terms agreed by the parties. The School's authority over the child derives from the contract with the parents and its duties at law.

A parent is recognised by the common law as having the right to make decisions concerning the child's education and to bring up their child in the religion of their choice. In all States and Territories the age of majority is 18 years. For these reasons, one approach would be for the School to adopt the view that in many circumstances, the contract with the parents will govern their relationship with the child in relation to privacy, and thus consents given by parents will act as consents given on behalf of the child and notice to parents will act as a notice given to the child.

However, this approach will not be appropriate in all circumstances. A School should recognise that young people do have rights under the Privacy Act and in some circumstances it would be appropriate to seek consents from them, particularly when they are aged 15 or over, as indicated by the APP Guidelines and ALRC. No doubt in most cases decisions whether to seek information or consents from students or from parents is likely to follow current practices. Thus, for example, where a student puts his or her name down to

take part in a team, the student would usually be impliedly consenting to it being disclosed to a relevant party to enable him or her to compete. As a student reaches greater maturity, the more important it will become to consider whether a parent should be asked for consent or the student. Hopefully in most cases common sense will provide the answer.

For example, in most cases it would be appropriate for the School to collect from a mature student personal (and sensitive) information about the student gained through an interview with the student. Also, there will be many instances throughout a student's schooling where it would be impracticable and inappropriate to first obtain a parent's consent when collecting personal information from a student (e.g. during day to day classroom activities). In respect of collecting personal information about students from parents, it is suggested that it is sufficient if parents are given a collection notice informing them of the requirements set out in APP 5.2, then students do not have to be specifically informed.

Another potential concern is that students may attempt to claim a right to prevent disclosure of personal information to a parent, such as their School report. The 'standard collection notice' seeks to overcome this by informing parents that the School will disclose personal information about a student to the student's parents. If a student attempted to restrict disclosure of personal information (such as a School report) to a parent, it is reasonably clear that this would be a permitted purpose as being a related purpose to the purpose for which the information was collected. This does not prevent the School exercising its discretion to restrict disclosure of the personal information.

Particular issues may arise in the context of information provided to staff members, including counsellors, by students 'in confidence' that is, where the student has asked or expected the staff member not to disclose it. One factor when considering how to deal with such situations will be the age and capacity of the students to provide or refuse consent.

Annexure B

Privacy Principles in Action

The Australian Privacy Principles

The Australian Privacy Principles are legal obligations under federal Privacy Laws. They apply to every Australian organisation and federal government agency that meets the qualifying criteria below:

- It has an annual turnover of more than $3 million;
- It provides a health service (which is broadly defined) to a person (even if the organisation's primary activity is not providing that health service);
- It trades in personal information (for example, buying or selling a mailing list);
- It is a contracted service provider under a Commonwealth contract (for example, an aged care provider or a disability services provider under a Commonwealth agreement);
- It is a credit reporting body;
- It operates a residential tenancy database;
- It is a reporting entity for the purposes of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act);
- It is an employee association registered or recognised under the Fair Work (Registered Organisations) Act 2009 (Cth);
- It is a business that conducts protection action ballots;
- It is a business prescribed by the Privacy Regulation 2013;
- It is related to a body corporate (for example, a subsidiary) that meets any of the above criteria (even if your not-for-profit itself does not); or
- It has opted into the Privacy Act (choosing to comply, despite not meeting any of the above criteria).

The Information Privacy Principles

The Information Privacy Principles are relevant for all Victorian public sector organisations, as well as some private or community sector organisations, where those organisations are carrying out functions under a State contract with a Victorian public sector organisation.

A State contract means a contract between an organisation (e.g. the Department of Education and Training) and a Contracted Service Provider [CSP] (e.g. an Approved Provider) under which services are provided by the CSP for the organisation (e.g. a funded Kindergarten Program).

The Health Privacy Principles

Victoria has specific Health Privacy Laws that provide a higher standard of protection of certain health information. Early Childhood Education and Care services collect, hold and use health information, therefore are required to follow the HPP under the Health Records Act, 2001.

Principles in Action

Organisations need to make sure their policy and procedures are consistent with all the Privacy Laws that apply to their organisation. If you're not sure, you should get legal advice.

The Child Information Sharing Scheme and Family Violence Information Sharing Scheme makes certain modifications to the Information Privacy Principles and the Health Privacy Principles to ensure that the scheme is able to operate as intended.

The table below is a reference tool that identities how all three legislations can work together and what it may look like in practice.

Australian Privacy Principles	Information Privacy Principles	Health Privacy Principles	Principles in action
APP 1 – Open and transparent management of personal information	IPP 5: Openness	Principle 5 Openness	Ballarat Grammar has an up to date *Privacy policy* that clearly sets out how we collect, use, disclose and store personal and health information. Stakeholders have access to this policy at any time, upon request.
APP 2 – Anonymity and pseudonymity	IPP 8: Anonymity	Principle 8 Anonymity	Wherever it is lawful and practicable, individuals and families will have the option of not identifying themselves when entering into transactions with Ballarat Grammar. This may include surveys, suggestion boxes, QIP feedback.
APP 3 Collection of solicited personal information and APP 4 – Dealing with unsolicited personal information	IPP 1: Collection IPP 10: Sensitive information	Principle 1 Collection	Ballarat Grammar will only collect the personal, sensitive and health information needed, and for which there is a purpose that is legitimate and related to the School's functions, activities and/or obligations. Personal, sensitive and health information about students and parents/guardians either in relation to themselves or a student enrolled at the service, will generally be collected via forms filled out by parents/guardians. This can include but not limited to Enrolment Records, Enrolment Application Forms, Medical Management Plans, Risk Minimisation Plans, Communication Plans, Attendance Records, Staff Records, Direct Debit Application Forms, Visitors Logbook. Other information may be collected from job applications, face-to-face interviews and telephone calls. Individuals from whom personal information is collected will be provided with a copy of the School's *Privacy Statement.* When Ballarat Grammar receives personal information from a source other than directly from the individual or the parents/guardians of the student concerned, the person receiving the information will notify the individual or the parents/guardians of the student to whom the information relates to. Ballarat Grammar will advise that individual of their right to share or not share this information with the source. Sensitive information will be collected only for the purpose of enabling the School to provide for the education and care of the student attending the School. **CISS & FVISS:** Information sharing entities are not obliged to collect personal or health information about an individual directly from that person if they are collecting the information from another information sharing entity under the scheme. If an information sharing entity collects personal or health information about a person from another information sharing entity under the scheme, it will not be obliged to take reasonable steps to notify that person that their information has been collected if doing so would be contrary to the promotion of the wellbeing or safety of a child. Information sharing entities will not be obliged to obtain consent from any person before collecting information under the scheme, including 'sensitive information' if they are sharing in accordance with the scheme.

APP 5 – Notification of the collection of personal information and APP 6 – Use or disclosure of personal information	IPP 2: Use and disclosure	Principle 2 Use and Disclose	Upon enrolment, commencement of employment, or any other time personal, sensitive or health information is collected, Ballarat Grammar will take reasonable steps to ensure individuals or families understand why this information is being collected, used, disclosed and stored. Individuals or families will be informed of the following: • Ballarat Grammar contact details; • The facts and circumstances of why personal, sensitive and health information is being collected; • What information is required by authorised law; • The purposes of collection; • The consequences if personal information is not collected; • Ballarat Grammar's usual disclosures of personal information; if applicable; and • Information about Ballarat Grammar's Privacy Policy. The following table identifies the personal, sensitive and health information that will be collected by Ballarat Grammar, the primary purpose for its collection and some examples of how this information will be used.

Personal, sensitive and health information collected in relation to:	Primary purpose of collection:	Examples of how the service will use personal and health, (including sensitive) information include:
Students and parents/ guardians	• To enable the service to provide for the education and care of the child attending the School • To promote the service	• Day-to-day administration and delivery of service. • Provision of a place for their child in the School. • Duty rosters. • Looking after children's educational, care and safety needs. • For correspondence with parents/guardians relating to their child's attendance. • To satisfy the service's legal obligations and to allow it to discharge its duty of care. • Visual displays in the service. • Newsletters. • Promoting the School through external media, including the School's website
The Board of Directors	• For the management of the service	• For communication with, and between, the Board members, employees and members of the association. • To satisfy the School's legal obligations.
Job applicants, employees, contractors, volunteers and students	• To assess and (if necessary) to engage the applicant, employees, contractor, volunteers or students, as the case may be • To administer the employment, contract or placement	• Administering the individual's employment, contract or placement, as the case may be. • Ensuring the health and safety of the individual. • Insurance. • Promoting the School through external media, including the School's website

The service may disclose some personal and/or health information held about an individual to:

- Government departments or agencies, as part of its legal and funding obligations;
- Local government authorities, in relation to enrolment details for planning purposes;
- Organisations providing services related to staff entitlements and employment;
- Insurance providers, in relation to specific claims or for obtaining cover;

			• Law enforcement agencies; • Health organisations and/or families in circumstances where the person requires urgent medical assistance and is incapable of giving permission; • Anyone to whom the individual authorises the service to disclose information. Sensitive information will be used and disclosed only for the purpose for which it was collected, unless the individual agrees otherwise, or where the use or disclosure of this sensitive information is allowed by law.
APP 7 – Direct marketing	N/A	N/A	A service must not use or disclose personal information it holds for the purpose of direct marketing. Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services.
APP 8 – Cross-border disclosure of personal information	IPP 9: Transborder data flows	Principle 9 Transborder Data Flows	Ballarat Grammar will only transfer personal of health information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme.
APP 9 – Adoption, use or disclosure of government related identifiers	IPP 7: Unique identifiers	Principle 7 Identifiers	Ballarat Grammar will not adopt, use or disclose a government related identifier unless an exception applies. The service will collect information on the following identifiers including but not limited to: • Information required to access the *Kindergarten Fee Subsidy* for eligible families; • Tax file number for all employees, to assist with the deduction and forwarding of tax to the Australian Tax Office – failure to provide this would result in maximum tax being deducted; • Medicare number: for medical emergencies; • For childcare services only: Customer Reference Number (CRN) for children attending childcare services to enable the family to access the Commonwealth Government's Child Care Subsidy (CCS) – failure to provide this would result in parents/guardians not obtaining the benefit.
APP 10 – Quality of personal information	IPP 3 - Data quality	Principle 3 Data quality	Ballarat Grammar will take reasonable steps to ensure that the personal and health information it collects is accurate, up-to-date and complete, as outlined in this Privacy policy. Ballarat Grammar will ensure any updated or new personal and/or health information is promptly added to relevant existing records and will send timely reminders to individuals or families to update their personal and/or health information to ensure records are up to date at all times. This can include but not limited to emergency contact details, authorised nominees, medical management plans, banking details, Working with Children Checks, VIT registration.
APP 11 – Security of personal information	IPP 4 - Data security	Principle 4 Data Security and Data Retention	Ballarat Grammar takes active measures to ensure the security of personal, sensitive and health information it holds, and takes reasonable steps to protect the stored information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Ballarat Grammar will also take reasonable steps to destroy personal and health information and ensure it is de-identified if it no longer needs the information for any purpose as described in the relevant regulations. In

			disposing of personal, sensitive and/or health information, those with authorised access to the information will ensure that it is either shredded or destroyed in such a way that the information is no longer accessible.
			
			Ballarat Grammar will ensure that, in relation to personal, sensitive and health information:
			• Access will be limited to authorised staff, the Approved Provider or other individuals who require this information in order to fulfil their responsibilities and duties;
			• Information will not be left in areas that allow unauthorised access to that information;
			• All materials will be physically stored in a secure cabinet or area;
			• Computerised records containing personal or health information will be stored safely and secured with a password for access;
			• There is security in transmission of the information via email, telephone, mobile phone/text messages, as detailed below:
			  ○ Emails will only be sent to a person authorised to receive the information;
			  ○ Faxes will only be sent to a secure fax, which does not allow unauthorised access; and
			  ○ Telephone – limited and necessary personal information will be provided over the telephone to persons authorised to receive that information; and
			• Transfer of information interstate and overseas will only occur with the permission of the person concerned or their parents/guardians.

APP 12 – Access to personal information and APP 13 – Correction of personal information	IPP 6 - Access and correction	Principle 6 Access and Correction	Individuals or families have the right to seek access to their own personal information and to make corrections to it if necessary. Upon request Ballarat Grammar will give an individual or families access to their personal or health information it holds are part of School operations in a timely manner. Ballarat Grammar must be satisfied through identification verification, that a request for personal or health information is granted. <u>Process for considering access requests</u> A person may seek access, to view or update their personal or health information: • If it relates to their child, by contacting the Nominated Supervisor; • For all other requests, by contacting the Approved Provider/secretary. Personal information may be accessed in the following way: • View and inspect the information; • Take notes; • Obtain a copy (scanned or photographed). Individuals requiring access to, or updating of, personal information should nominate the type of access required and specify, if possible, what information is required. The Approved Provider will endeavour to respond to this request within 45 days of receiving the request. The Approved Provider and employees will provide access in line with the privacy legislation. If the requested information cannot be provided, the reasons for denying access will be given in writing to the person requesting the information.

			In accordance with the legislation, the School reserves the right to charge for information provided in order to cover the costs involved in providing that information. The privacy legislation also provides an individual about whom information is held by the service, the right to request the correction of information that is held. The service will respond to the request within 45 days of receiving the request for correction. If the individual is able to establish to the service's satisfaction that the information held is incorrect, the service will endeavour to correct the information. There are some exceptions set out in the *Privacy and Data Protection Act 2014,* where access may be denied in part or in total. Examples of some exemptions are where: • The request is frivolous or vexatious; • Providing access would have an unreasonable impact on the privacy of other individuals; • Providing access would pose a serious threat to the life or health of any person; • The School is involved in the detection, investigation or remedying of serious improper conduct and providing access would prejudice that.
N/A	N/A	Principle 10 Transfer or closure of the practice of a health service provider	N/A
N/A	N/A	Principle 11 Making information available to another health service provider	N/A

Annexure C

Privacy Statement

We believe your privacy is important.

Ballarat Grammar has developed a *Privacy Policy* that illustrates how we collect, use, disclose, manage and transfer personal information, including health information. This policy is available on request.

To ensure ongoing funding and licensing, our service is required to comply with the requirements of privacy legislation in relation to the collection and use of personal information. If we need to collect health information, our procedures are subject to the *Health Records Act 2001*.

The Child Information and Family Violence Information Sharing Scheme allows Early Childhood Services to freely request and share relevant information with Information Sharing Entities to support a child or group of children's wellbeing and safety when the threshold test has been met.

Purpose for which information is collected

The reasons for which we generally collect personal information are given in the table below.

Personal information and health information collected in relation to:	**Primary purpose for which information will be used:**
Children and parents/guardians	To enable us to provide for the education and care of the child attending the School. To manage and administer the service as required.
The Board of Directors	For the management of the service. To comply with relevant legislation requirements.
Job applicants, employees, contractors, volunteers and students	To assess and (if necessary) to engage employees, contractors, volunteers or students. To administer the individual's employment, contracts or placement of students and volunteers.

Please note that under relevant privacy legislation, other uses and disclosures of personal information may be permitted, as set out in that legislation.

Disclosure of personal information, including sensitive and health information

Some personal information, including health information, held about an individual may be disclosed to:

- Government departments or agencies, as part of our legal and funding obligations;
- Local government authorities, for planning purposes;
- Organisations providing services related to employee entitlements and employment;
- Insurance providers, in relation to specific claims or for obtaining cover;
- Law enforcement agencies;
- Health organisations and/or families in circumstances where the person requires urgent medical assistance and is incapable of giving permission;
- Anyone to whom the individual authorises us to disclose information; and/or
- Information sharing entities to support a child and a group of children's wellbeing and safety.

Laws that require us to collect specific information

The Education and Care Services National Law Act 2010 and the *Education and Care Services National Regulations 2011, Associations Incorporation Reform Act 2012 (Vic)* and employment-related laws and agreements require us to collect specific information about individuals from time-to-time. Failure to provide the required information could affect:

- A child's enrolment at the School;
- A person's employment with the School; and/or
- The ability to function as an incorporated association.

Access to information

Individuals about whom we hold personal, sensitive or health information can gain access to this information in accordance with applicable legislation. The procedure for doing this is set out in our *Privacy Policy*, which is available on request.

For information on the *Privacy Policy*, please refer to Nexus, the School's website, or contact the School directly.

Annexure D

Permission Form for Photographs and Videos

Background information
Photographs and videos are classified as 'personal information' under the *Privacy and Data Protection Act 2014*.
The purpose of this permission form is to:

- Notify parents/guardians as to who will be permitted to take photographs/videos, where these will be taken and how they will be used.
- Comply with the privacy legislation in relation to all photographs/videos taken at the service, whether by the Approved Provider, Nominated Supervisor, Persons in Day-to-Day Charge, educators, staff, parents/guardians, volunteers or Students on placement.
- Enable photographs/videos of students to be taken as part of the program delivered by the service, whether group photos, videos or photos at special events and excursions etc.

Photographs/videos taken by staff.
Staff at the service may take photographs/videos of children as part of the program. These may be displayed at the service, on the Ballarat Grammar website/social media platforms or placed in the School's publications or promotional material to promote the School, or for any other purpose aligned to the School's business operations. Some staff may use learning journals in which photographs are included.

When the photographs/videos are no longer being used, the School will destroy them if they are no longer required, or otherwise store them securely at the School. It is important to note that while the School can nominate the use and disposal of photographs they organise, the School has no control over those photographs taken by parents/guardians of children attending the program or activity.

Group photographs/videos taken by parents/guardians.
Parents/guardians may take group photographs/videos of their own child/children at special service events such as birthdays, excursions and other activities. Parents must ensure that where the photographs/videos include other children at the service they are sensitive to and respectful of the privacy of those children and families in using and disposing of the photographs/videos.

Photographs taken by a photographer engaged by the School.
A photographer may be engaged by the service to take individual and/or group photographs of students. Information will be provided in written form to parents/guardians prior to the event, and will include the date and the photographer's details.

Photographs/videos for use in newspapers, Ballarat Grammar website and other external publications.
The permission of parents/guardians of students will, on every occasion, be obtained prior to a student's photograph being taken to appear in any newspaper/media or external publication, including the School's newsletter, publications and website.

Photographs/videos taken by Students on placement.
Students at the School may take photographs/videos of student as part of their placement requirements.

Access to photographs/videos.
Access to any photographs or videos, like other personal information, is set out in the service's *Privacy Policy,* which is displayed at the service and available on request.

Confirmation of consent

I consent/do not consent to the arrangements for the use of photographs and/or videos, as stated in this permission form.

Parent's/guardian's name _____

Student's name _____

Signature (parent/guardian) _____ Date _____

Annexure E

SHARING INFORMATION UNDER THE CISS AND FVISS

Applying the threshold test

Before sharing information with other Information Sharing Entities (ISE)'s the threshold test requirements must be meet.

The requirements for sharing are different depending on the purpose of the sharing, if sharing for both purposes (Child Wellbeing or Safety and/or Family Violence), you must meet the requirements of each of the schemes.

Although child wellbeing and safety takes precedence over an individual's privacy, privacy must still be protected through careful and selective information sharing.

Threshold requirements for the Child Information Sharing Scheme:

1	The information sharing entity is requesting or disclosing confidential information about any person for the purpose of promoting the wellbeing or safety of a child or group of children; and
2	The **disclosing** information sharing entity reasonably believes that sharing the confidential information may assist the receiving information sharing entity to carry out one or more of the following activities: • Make a decision, an assessment or a plan relating to a child or group of children; • Initiate or conduct an investigation relating to a child or group of children; • Provide a service relating to a child or group of children; • Manage any risk to a child or group of children; and
3	The information being **disclosed** or **requested** is not known to be 'excluded information' under Part 6Aof the Child Wellbeing and Safety Act (and is not restricted from sharing by another law), information that could: • Endanger a person's life or result in physical injury; • Prejudice a police investigation or interfere with the enforcement or administration of the law; prejudice a coronial inquest; prejudice a fair trial of a person; • Be legally privileged; • Reveal a confidential police source; • Contravene a court order; • Be contrary to the public interest; or • Information sharing would contravene another law.

Threshold requirements for the Family Violence Information Sharing Scheme:

1	**The purpose of sharing is to assess family violence risk OR protect victim survivors from family violence risk.** There are two purposes for which information can be shared between ISEs: • Family violence assessment purpose: The purpose of establishing or assessing the risk of a person committing family violence or being the subject of family violence. This would include: ○ Establishing family violence risk;

	○ Assessing the risk to the victim survivor; ○ Correctly identifying the perpetrator. • Family violence protection purpose: Once family violence risk is established, to manage the risk to the victim survivor. This includes information sharing to support ongoing risk assessment.
2	**The applicable consent requirements are met.** Is the consent required when a child is at risk of family violence? • Consent is not required from any person to share information relevant to assessing or managing family violence risk to a child. However, you should seek the views of the child and non-violent family members where it is safe, reasonable and appropriate to do so. • Where a student is 18 years of age or older, they are an adult and so you may need their consent to share their information, or the information of third parties, unless you can legally share under existing privacy laws or when there is a child at risk. • In situations where an adolescent is using family violence against an adult family member, you may need the consent of the adult victim survivor to share their information.
3	**The information is not excluded information.** Excluded information is information that could: • Endanger a person's life or result in physical injury; • Prejudice a police investigation or interfere with the enforcement or administration of the law, prejudice a coronial inquest, prejudice a fair trial of a person, be legally privileged; • Reveal a confidential police source; • Contravene a court order; • Be contrary to the public interest; • Information sharing would contravene another law.

Making a request to another Information Sharing Entity

Before disclosing information under the Child Information Sharing Scheme and Family Violence Information Sharing Scheme, it is important that information sharing entities take reasonable care to verify the identity of the professional or service and ensure that they are an information sharing entity.

- The ISE list is a searchable database that can be used to identity organisation and services prescribed under the CISS and FIVSS.
- Before making a request, check to see if the organisation is a prescribed entity via the Access the ISE list.
- Refer to Information Sharing Entity List Uses Guide on how to navigate the database.
- ISEs should respond to requests for information in a timely manner, including when they are declining to provide information in response to the request.
- If an ISE is declining a request from another ISE, they are required to provide written reasons for doing so.

Making a request or receiving a request under the Child Information Sharing Scheme

An ISE may request information when it meets the first and third parts of the threshold. That is, the information being requested is:

- To promote the wellbeing or safety of a child or group of children
- Not excluded information under the Child Information Sharing Scheme to their knowledge.

ISE should use professional judgement to decide which organisation or service to request information from, taking into account the following:

- The activity the requesting information sharing entity is seeking to undertake and the type of information that may assist them;
- The roles and responsibilities of other information sharing entities and the information they are likely to hold;
- The currency and relevance of the information other information sharing entities are likely to hold.

The ISE requesting the information should provide sufficient detail to enable the responding ISE to make a decision about whether all three parts of the threshold have been met, in order to assist them to:

- Identify relevant information to respond to the request;
- Form an opinion about whether the information may be disclosed under the CISS (whether the disclosure meets the threshold).

When making a request, an ISE may disclose any confidential information that may assist the responding ISE to:

- Identify the information they hold that is relevant to the request;
- Form an opinion on whether the information may be disclosed under the scheme.

If the legal requirements (or threshold) of the scheme are met, an ISE:

- **May** make requests for information to another ISE;
- **Must** disclose relevant information to another ISE, if requested;
- **May** disclose information voluntarily (proactively) to other ISEs.

ISEs will use their expertise and exercise their professional judgement to identify:

- The range of needs and risks that impact on a child's life to inform a decision as to whether the threshold is met.
- What and how much information to share.
- Who to share with to support improved service delivery and promote the wellbeing or safety of the child or children.

Making a request or receiving a request under the Family Violence Information Sharing Scheme

Under Part 5A of the *Family Violence Protection Act 2008* (FVPA), ISEs may request or share information with other ISEs about a person that is relevant to assessing or managing a family violence risk. The information may relate to a victim survivor (adult or child), alleged perpetrator/perpetrator or third party.

Only information that is **relevant** to assessing or managing a risk of family violence can be shared under the Scheme. In determining what information is relevant, practitioners should use their professional judgement and refer to the *Family Violence Policy*.

Where an ISE receives a request, it **must** share that information, either verbally or in writing, provided that the information meets the requirements (the threshold) of the Scheme. The onus is on the ISE sharing information to ensure that they are disclosing information about a person in accordance with the law. There is no restriction on an ISE making a request.

If there is no existing relationship with the ISE the information is being requested from, verification may need to take place (e.g. by sending an email with the entity's official account).

There are **two purposes** for which ISEs can share information with each other under the FVPA, Part 5A:

a. For family violence assessment purposes
   - Only prescribed risk assessment entities (RSE) are entitled to make requests and receive information for a family violence assessment purpose, which focuses on identifying who the 'actual' perpetrator and victim survivor are and establishing the level of risk the perpetrator poses to the victim survivor.

   OR

b. For family violence protection purposes
   - Any prescribed ISE is permitted to request and receive information for a family violence protection purpose. The focus at this stage is about managing the risk of the perpetrator committing family violence or the victim survivor being subjected to family violence. This could include information sharing as part of ongoing risk assessment.

Once it has been established which purpose the information is to be exchanged, ensure that:
- Sufficient information is provided to the ISE to help them identify what information they hold that might be relevant and whether they should disclose that information.
- The purpose of the information is clearly identified and why it is believed the information is relevant.
- Precedence is given to a victim survivor's right to be safe from family violence when discussing relevant information.
- Record keeping is completed, including the name of the service that was contacted, the name of the ISE and the information that was disclosed.
- Any risk assessment or safety plan are documented, as a result of the information sharing.
- Information is used only for a purpose permitted by law.
- If information request is refused, record this refusal in writing and keep this refusal on file.

Sharing information for risk assessment

Once a reasonable belief has been established that family violence risk is present and the identity of the perpetrator or victim survivor/s are clear (e.g. the victim survivor has identified the perpetrator), this would enable any ISE to make referrals for specialist services or professionals to complete a comprehensive family violence risk assessment. Some of these specialist services are prescribed as Risk Assessment Entities (RAEs).

ISEs can share relevant information proactively or on request with RAEs for risk assessment purposes. That is, in order to:
- Confirm whether family violence is occurring;
- Enable RAEs to assess the level of risk the perpetrator poses to the victim survivor;
- Correctly identify the perpetrator who is using family violence.

Family violence risk assessment is an ongoing process and is required at different points in time from different service perspectives. Education and care services will have a role in working collaboratively with other services to contribute to ongoing risk assessment and management of family violence.

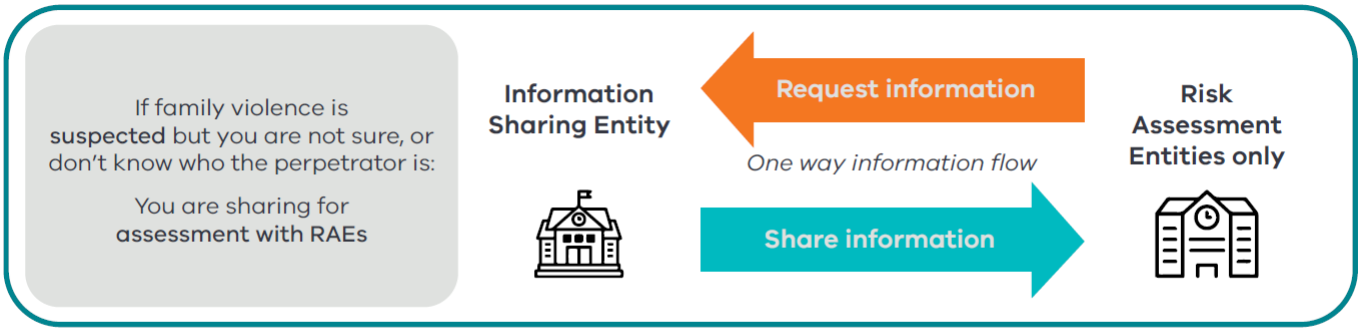

Figure 1: Overview of activities when sharing information for risk assessment

Victoria State Government, 2021. *Information Sharing and Family Violence Reforms Contextualised Guidance*. Melbourne, p.38.

SEs can only share information with other ISEs that are not RAEs. Request information from RAEs once family violence risk is established and the identity of the perpetrator and victim survivors are known. This is to prevent sharing that might escalate risk to a child or family member.

Sharing for risk management (protection):

Once family violence is established, ISEs can share proactively with other ISEs and request information, including from RAEs, if they reasonably believe sharing is necessary to:

- Remove, reduce or prevent family violence risk;
- Understand how risk is changing over time;
- Inform ongoing risk assessment.

This opens a two-way flow of information that enables ISEs to form a complete picture of risk and collaborate to support children and families experiencing family violence.

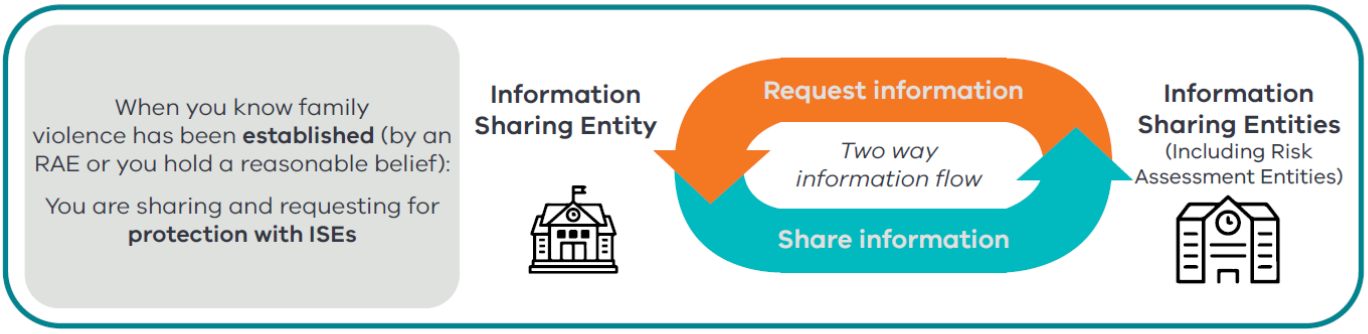

Figure 2: Overview of activities when sharing information for risk management (protection)

Victoria State Government, 2021. *Information Sharing and Family Violence Reforms Contextualised Guidance*. Melbourne, p.39.

When making a request, ensure you are speaking with someone suitably trained to use Part 5A of the Family *Violence Protection Act 2008* (FVPA).

Table 1

Information Sharing Entities that are also Risk Assessment Entities	
▪ State-funded specialist family violence services (including refuges, Men's Behaviour Change Programs, family violence counselling and therapeutic programs) ▪ Risk Assessment and Management Panel (RAMP) members (including those services that would not otherwise be prescribed but only when participating in a RAMP) ▪ State-funded sexual assault services	▪ Child Protection ▪ Child FIRST services (excluding broader family services) ▪ Victims Support Agency (including Victim Assistance Programs and Victims of Crime Helpline) ▪ Victoria Police ▪ The Orange Door services.
Information Sharing Entities	
▪ Magistrates' Court of Victoria officials ▪ Children's Court of Victoria officials ▪ Corrections Victoria and Corrections-funded services ▪ Adult Parole Board ▪ Youth Justice (including the Secretariat to the Youth Parole Board) and Youth Justice funded services ▪ Multi-Agency Panels to Prevent Youth Offending ▪ Justice Health and funded services ▪ State-funded sexually abusive behaviour treatment services ▪ State-funded perpetrator intervention trials ▪ Registered community-based child and family services	▪ Maternal and Child Health ▪ Registered out of home care services ▪ Department of Families, Fairness and Housing ▪ State-funded homelessness accommodation or homelessness support services providing access point, outreach or accommodation services ▪ Designated mental health services ▪ State-funded alcohol and other drug services ▪ Tenancy Advice and Advocacy Program ▪ State-funded financial counselling services ▪ Commission for Children and Young People ▪ Disability Services Commissioner.

Record keeping

ISEs have specific record keeping obligations under the FVISS and the CISS. ISEs can choose how they will meet their record keeping obligations, which might include written or online case notes, specific record keeping forms or IT solutions, and are in line with the *Privacy and Data Protection Act 2014 (Vic)* and, where applicable, the Australia Privacy Principles obligations.

When an ISE receives a request to share information they must record:
- The ISE that requested the information;
- The date of the request;
- The information that was requested; and
- If refusing a request, the request and the reason why it was refused.

When an ISE shares information (either proactively or on request) they should:
- Know and record what scheme they are sharing under (FVISS, CISS or both);
- Know and record whom information is being shared about;
- Record how the threshold for sharing was met; and
- Relevant risk assessments or safety plans that have been prepared for a person at risk of family violence.

Documentation is also required if sharing about:

- Adult victim survivors of family violence or third parties under FVISS (where a child is at risk);
- A child's parent under CISS;
- Child victim survivors of family violence;
- Any child in order to promote their wellbeing or safety;
- Whether their views were sought about sharing their information;
- If their views were not sought, record the reason why;
- If they were informed that their information was shared;
- Whether information was shared with consent and whether the consent was written, verbal or implied;
- If the information was shared without consent, record the reason why;
- If the information was shared without consent, record if the person was informed that their information was shared without consent.

Examples of record keeping forms can be found at: www.vic.gov.au/guides-templates-tools-for-information-sharing

Handling information sharing and risk assessment complaints under the CISS and FVISS

Types of complaints
ISEs may receive complaints from:

1. Individuals in relation to privacy breaches, for example the ISE has:
   - Misidentified an adult victim survivor as a perpetrator and shared information about them without consent.
   - Shared information that is not relevant to the purpose for which it was shared.
2. Individuals in relation to any other conduct under the Schemes, for example the ISE has:
   - Not sought the views of a child and/or relevant family member and the complainant believes it was reasonable, safe and appropriate to do so.
   - In the view of the complainant, failed to foster positive relationships between a child and significant people in the child's life, in the way they applied the Schemes.
3. Other ISEs in relation to how the ISE is sharing information under the Schemes. For example, an ISE may make a complaint about:
   - Another ISE refusing to share relevant information that should be shared.
   - The timeliness of responses.

Complaints record keeping

The following information must be recorded if a complaint is received under the Schemes:

- Date the complaint was made and received;
- Nature of the complaint;
- Action taken to resolve the complaint;
- Action taken to lessen or prevent the issue from recurring;
- Time taken to resolve the complaint; and
- If the complaint was not resolved, further action that was taken.

Note: Accepted standard practice is that a response should be provided within 30 days of receiving the complaint. All complaints must be handling according to the *Privacy and Data Protection Act 2014 (Vic)* and, where applicable, the Australia Privacy Principles.