



Privacy Protection Policy & Procedure

1. Purpose

The purpose of this policy is to establish a structured framework for the collection, use, storage, disclosure, protection and management of personal and sensitive information at Princeton International College.

Princeton International College is committed to managing personal and sensitive information in a lawful, fair, transparent and secure manner and to implementing appropriate privacy, confidentiality and information security practices across all operational areas. The College recognises the importance of protecting student, staff and stakeholder information from misuse, interference, loss, unauthorised access, modification or disclosure and maintaining secure digital, electronic and cloud-based information management practices.

This policy ensures that Princeton International College:

- complies with the Privacy Act 1988, Australian Privacy Principles (APPs), ESOS Act 2000, National Code of Practice for Providers of Education and Training to Overseas Students 2018, Standards for Registered Training Organisations (RTOs) 2025 and other applicable legislative requirements
- establishes clear controls for information access, storage, handling, retention and disposal
- ensures personal information collected from overseas students is managed in accordance with CRICOS and ESOS framework requirements
- supports accurate regulatory reporting, student administration, governance and operational integrity
- promotes staff awareness, accountability and consistent information handling practices across the organisation

2. Definitions

- **Personal information** means information or opinions that can identify or reasonably identify an individual. This includes an individual's name, signature, address, phone number, date of birth, employee record information, photographs, internet protocol (IP) addresses, biometric data like voice prints and facial recognition (as they capture unique characteristics of a person), and location data from mobile devices, which can disclose patterns or habits of user activity. It is important to note that personal information also includes sensitive information and credit information (see below).

Privacy Protection Policy & Procedure

- Although not specifically defined within the Privacy Act personal information should also be taken to include information that is used to verify the identity of a person when collected to establish their eligibility for a training subsidy or to assist them to create a unique student identifier. This can include what is often referred to as “high risk personal information” which includes information such as drivers licence details, passport details, birth certificate, rates notice, Medicare Card details, Visa details, etc. When combined with other personal information which may be publicly available on social media or through the internet, access to high risk personal information carries heightened risks including the risk of identity theft.
- **Sensitive information** means personal information or opinions concerning an individual's racial or ethnic origin, political opinions, political association memberships, religious beliefs or affiliations, philosophical beliefs, memberships of professional or trade associations, trade union memberships, sexual preferences or practices, criminal records, health information, genetic information that does not constitute health information, biometric information intended for automated biometric verification or identification, and biometric templates.
- **Credit information** means specific details collected and used to evaluate an individual's creditworthiness. This includes the full name, date of birth, sex, current or last known address, previous two addresses, current or last known employer's name, driver's licence number, and information about credit providers that have extended consumer credit to a person, including whether they're licensed by ASIC. It also includes details about the type and terms of consumer credit provided, dates of credit availability and termination, credit limits, repayment obligations, repayment history (including timely or missed payments and financial hardship records), and information regarding credit enquiries made by providers in response to a person's credit applications. Credit information further encompasses records of defaults on payments of \$150 or more, statements acknowledging payments previously in default, variations or new credit arrangements resulting from defaults, court judgments related to a person's credit, information recorded on the National Personal Insolvency Index (including bankruptcy and debt agreements), publicly available details regarding a person's creditworthiness, and opinions by credit providers about serious credit infringements a person may have committed.

3. Policy Statement

Princeton International College collects and stores personal and sensitive information relating to its students, staff, education agents, employers and other stakeholders. In doing so, Princeton



Privacy Protection Policy & Procedure

International College has implemented this policy to comply with its obligations under the Privacy Act 1988, Australian Privacy Principles (APPs), the ESOS Act 2000, and the National Code 2018.

Protecting personal and sensitive information is essential not only to ensure compliance with legislative requirements but also to safeguard Princeton International College staff and students, including overseas students, from potential financial, legal, or reputational harm. Mishandling personal and sensitive data can lead to breaches of trust, significant reputational damage, and potential loss of enrolments, business partners, and revenue. Additionally, losing or compromising critical information may impact the College's ability to deliver quality training and assessment services.

Implementing robust information security practices provides significant operational benefits, including improved efficiency, stronger data integrity, and reduced risk of privacy breaches. These practices also support Princeton International College in meeting its regulatory reporting obligations (including AVETMISS and PRISMS) and ensure that personal and sensitive information is handled responsibly and securely at all times.

3.1 Authority to collect and store information

Princeton International College is an approved Registered Training Organisation (RTO) registered with the Australian Skills Quality Authority (ASQA). This registration is issued under the authority of the National Vocational Education and Training Regulator Act 2011. This legislation requires Princeton International College to collect personal and sensitive information from our students. This requirement is specified in the *Data Provision Requirements 2020* which is one of the legislative instruments that Princeton International College must comply with as a condition of its registration.

The *Data Provision Requirements 2020* require Princeton International College to collect data from students in accordance with the Australian Vocational Education Training Information Statistical Standard (AVETMISS). This is a complex information standard that defines information about who the student is, where the training is delivered and what they are studying. The Compliance Standards for RTOs require Princeton International College to retain and manage records in accordance with legislative and regulatory retention requirements and to report training activity to government agencies in accordance with mandatory reporting requirements.

In addition to the *Data Provision Requirements 2020*, the *Student Identifiers Act 2014* also requires Princeton International College to collect high risk personal information for the purpose of creating or verifying a student's Unique Student Identifier. Together, these requirements form a statutory obligation to collect, store and report information of any student participating in nationally recognised training with Princeton International College.

3.2 Use of personal information

To comply with its obligations under the *Data Provision Requirements 2020*, the *Student Identifiers Act 2014*, or contractual obligations or to facilitate an outcome of a service offered to students, Princeton International College will use personal information to comply with reporting obligations to Government agencies at the Commonwealth level and if accessing Government subsidised training also with a relevant State or Territory Government agency. Under some circumstances such as to facilitate an outcome of a service (such as licencing), Princeton International College may also need to report personal information to other relevant Government or responsible agencies. Students enrolling into a course with Princeton International College are advised of our collection and use of personal information with the *Student Handbook* sections related to “*Your Privacy*” and “*National VET Data Policy*”.

3.3 Solicited information

Contact information such as name, organisation, position, address, telephone, and email are collected for marketing, support services, mandatory reporting and for communicating with stakeholders as part of our day-to-day operation.

In addition to the collection of training activity information, Princeton International College will also collect, store and report information relating to satisfaction surveys, complaint handling and on our client employers.

Names, addresses, phone numbers, emergency contact details, bank account details and other employment related information is collected from employees for the purpose of managing human resources. The management of staff personal information complies with this policy.

3.4 Sensitive information

Personal information collected by Princeton International College that may be regarded as ‘sensitive’ under the Privacy Act includes:

- ‘Disability’ and ‘long-term impairment status’ (health); and ‘indigenous status’, ‘language spoken at home’, ‘proficiency in spoken English’, ‘country of birth’ (implies ethnic/racial origin). This information is specified in the AVETMISS data elements and is collected for the national VET data collections, national VET surveys, and may be collected for VET-related research.

Privacy Protection Policy & Procedure

- ‘Dietary requirements’ (health-related) are collected for event catering purposes only.
- Biographical information, which may contain information on ‘affiliations’ and ‘membership of a professional or trade association’ are obtained from keynote speakers for event marketing purposes.
- ‘Memberships of professional associations’ and ‘health and work injury information’ is collected from Princeton International College employees for HR management purposes.

3.5 Direct marketing

Princeton International College respects an individual’s right not to receive marketing material and provides an option within communications and on its website for individuals to unsubscribe from receiving marketing material. Princeton International College conducts its marketing communications and dissemination of service information in accordance with Australian Privacy Principle 7 (Direct marketing), the Spam Act 2003 (in respect of electronic communications), and the Do Not Call Register Act 2006. Princeton International College does not engage in unsolicited marketing practices. Princeton International College is not to undertake in unsolicited marketing practices, ever.

3.6 Unsolicited personal information

Unsolicited personal information is information Princeton International College may receive without actively asking for it. If Princeton International College should receive unsolicited personal information, it will be treated and managed according to the APPs. This means Princeton International College will need to assess the information to determine if holding the information is lawful. This includes assessing if the information could have been collected if actively sought by Princeton International College in the first place in accordance with Australian Privacy Principle 3 (Collection of Solicited Personal Information) and, is it necessary for Princeton International College to hold the information to perform its function and service to students? If the answer to either of these questions is no, Princeton International College is to destroy or de-identify the information as soon as practicable and inform the owner of the information of the actions.

The following is a practical example of protecting unsolicited personal information: A parent of a student sends an email to Princeton International College with records of their young adult son’s medical history and condition. Princeton International College did not request this information and

Privacy Protection Policy & Procedure

does not require it for any reasonable purpose in providing services to the student. In this scenario, the Administration Officer in consultation with the CEO, should promptly evaluate the information. This evaluation would determine that Princeton International College could not have lawfully collected private medical information, it must securely destroy or de-identify the information as soon as possible and advise the parent and student of this action.

3.7 Notification of collection

Princeton International College aims to notify individuals of the collection of their personal information before, or at the time of collection, or as quickly as possible thereafter. Notifications are usually in writing but may be verbal by phone. Examples of notification include:

- Marketing – notification is provided on our website course application page. Individuals are also notified at the time of collecting personal information for events. A privacy notice is provided in all Princeton International College marketing communications.
- Pre-enrolment information supplied to the prospective student prior to their enrolment or commencement includes the Student Handbook. Students enrolling into a course with Princeton International College are advised of our collection and use of personal information with the *Student Handbook* sections related to “Your Privacy” and “National VET Data Policy”.
- Quality Indicator surveys – notification is provided in the email of invitation to participate in the surveys and also at the time of collecting the information.
- Princeton International College staff – Notification is provided on employment commencement.

3.8 Disclosure of personal information

Princeton International College is not to disclose personal information other than for the purpose for which it was collected, or an individual has consented to a secondary purpose, or an individual would reasonably expect this (such as receiving communications about upcoming events), or if required by law.

Princeton International College may share personal information with the Commonwealth government in accordance with Commonwealth contractual or regulatory obligations. In these circumstances, Princeton International College will take reasonable steps to inform and seek consent from the individuals concerned and take all reasonable steps to ensure that the recipient handles the personal information according to the APPs.



Privacy Protection Policy & Procedure

Princeton International College is not to sell or distribute mailing lists or student contact information to third parties under any circumstance. Princeton International College does not disclose personal information to overseas recipients. While people around the world can access material published on our website, no publications on our website are to contain identifiable personal information.

Princeton International College may disclose personal information of overseas students to the Australian Government and designated authorities, including through PRISMS, where required under the ESOS Act 2000 and National Code 2018.

3.9 Management of personal information

Princeton International College will ensure the personal information it collects and uses or discloses is accurate, up to date, complete and relevant. Princeton International College routinely updates the information held in its student management system. This includes confirming with students who are returning for a new enrolment if their personal contact details have changed.

The College ensures that student information used for course progress monitoring, attendance, and visa compliance is accurate and up to date.

3.10 Access to and correction of personal information

Individuals may, subject to the exceptions prescribed by the APPs, request access to and correction of their personal information where this is collected directly from individuals by Princeton International College.

Princeton International College does not charge for giving access to or for correcting personal information unless the student is requesting copies to be made of information which may incur an administrative fee (Refer to *Records Management Policy and Procedure*). Requests for access to or correction of personal information should be made in accordance with the access to records arrangements outlined in the *student Handbook* and *Records Management Policy and Procedure*

3.11 Retention and recording of high-risk personal information

In accordance with the *APPs principles 11.2* and *Student Identifiers Act 2014*, section 11, Princeton International College is not to continue to hold information where it has no further purpose for this information. An example of this may include high risk personal information (refer to definitions) which may include a copy of a student passport, drivers' licence or Medicare Card. Once the

Privacy Protection Policy & Procedure

student's identification or eligibility has been verified (the purpose), Princeton International College is to destroy through shredding or permanently deleting these records so that these records are no longer being stored by Princeton International College. Princeton International College's information security risk is significantly reduced if these records are destroyed as soon as possible after the purpose for collecting this information has been satisfied.

Where possible, staff should seek to confirm verification using high risk personal information directly with the student either in person or over video conference and avoid the need to collect and store these records altogether.

Princeton International College is to retain the details of high risk personal information that is used for the purpose of verification by recording the type of information that was viewed, the date it was viewed and by who. This is an acceptable record for the purpose of meeting our compliance obligations and is an effective risk avoidance strategy that is to be applied.

3.12 Information Security

Princeton International College applies strict security controls over all information collected and stored. The College operates a predominantly digital record management system, and all information security practices prioritise secure electronic and cloud-based storage.

Where hard copy records exist, these are minimised and managed in accordance with the same security principles.

i. Electronic and Digital Information Security (Primary Method)

The following strategies apply to the storage and handling of electronic information:

- All records are stored within secure systems, including the Student Management System and authorised cloud-based platforms
- Access to information is restricted to authorised personnel through role-based permissions
- Multi-factor authentication (MFA) is implemented where available
- Data is protected through encryption both in transit and at rest
- Regular backups are performed and securely maintained, including offsite storage
- Systems are regularly updated with security patches, antivirus protection, and firewall controls
- Staff must use secure passwords and must not share login credentials
- Access is revoked immediately upon staff separation or role change

Privacy Protection Policy & Procedure

- Electronic records must be capable of being retrieved and reproduced for audit, reporting, or student access purposes

ii. **Hard Copy Information Security (Where Applicable Only)**

Where hard copy records are temporarily created or required:

- Hard copy records must be minimised wherever possible
- Any physical documents must be stored securely to prevent unauthorised access
- Access to hard copy records is restricted to authorised personnel only
- Documents must not be left unattended in public or shared areas
- All sensitive documents must be securely destroyed (e.g. shredding) when no longer required
- Staff must follow clean desk practices to ensure information is not exposed

3.13 Information classification labels

Princeton International College applies information classification labels to support the secure handling, storage, access, disclosure and management of information across all operational areas. Information classification labels assist staff in identifying the sensitivity, confidentiality and operational importance of information and provide guidance regarding appropriate handling and security requirements.

The use of information classification labels supports Princeton International College in:

- protecting student, staff and organisational information from misuse, unauthorised access, modification, disclosure or loss
- maintaining compliance with the Privacy Act 1988, Australian Privacy Principles (APPs), ESOS Act 2000, National Code 2018, Standards for Registered Training Organisations (RTOs) 2025 and other applicable regulatory obligations
- supporting consistent information security and records management practices across VET, ELICOS and administrative operations
- reducing operational, legal, financial and reputational risks associated with information handling
- promoting staff accountability, confidentiality and secure information management practices

Privacy Protection Policy & Procedure

Information classification labels apply to both physical and electronic records, including records maintained within Wisenet, cloud-based systems, student files, assessment systems, financial systems, staff records and regulatory compliance records.

The CEO maintains overall responsibility for governance oversight relating to information classification, privacy management and information security practices. Authorised staff members, including Administration Staff, Student Support Officers, the Training Manager and ELICOS Coordinator, are responsible for ensuring information is handled, stored and accessed in accordance with the applicable classification requirements.

Information classification labels must be clearly identified on documents or records where applicable and must be managed in accordance with Princeton International College's information security, privacy and records management requirements.

Label	Description	Examples	Rules
Public	Information intended for public access, openly available internally and externally without restrictions.	Marketing brochures Website content Student Handbook	No special security measures required. May be shared externally without approval.
Internal Only	Information available only to Princeton International College employees or approved partners and not intended for public dissemination.	Policies and procedures Meeting minutes Internal correspondence Continuous improvement records Student engagement reports Validation records Staff meeting records	Distribute internally or to authorised partners only. Not for public disclosure without approval. Classification label must be applied where practical and appropriate.
Academic	Information created specifically for training, learning, or assessment purposes within or associated with Princeton International College.	Training manuals Course handbooks Assessment guidelines and resources	Distribute to students and trainers. May be shared externally with authorisation.

Privacy Protection Policy & Procedure

Label	Description	Examples	Rules
		Student workbooks and learning activities Training and assessment strategies ELICOS learning materials Assessment validation records Trainer assessment tools	Not intended for unrestricted public dissemination unless explicitly approved.
Confidential	Information that, if disclosed externally, could negatively impact business operations, reputation, or competitive advantage.	Business plan Financial performance information Contractual agreements Agent agreements Student complaints and appeals Rectification reports	Limit access to need-to-know basis. Secure storage and handling required. External sharing needs explicit authorisation. Classification label must be applied where practical and appropriate.
Restricted	Highly sensitive business information that could lead to serious financial, legal, or reputational damage if improperly disclosed.	Legal advice or litigation information Critical intellectual property ASQA audit documentation PRISMS access credentials Legal correspondence	Access restricted to explicitly approved personnel. Secure encryption and restricted access controls required. No external sharing without CEO authorisation. Classification label must be applied where practical and appropriate.
Private	Personal or sensitive staff or student information protected by privacy laws and internal policies.	Student personal information Staff personal information Payroll information	Compliance with privacy laws. Restricted access only to those who need to access to perform their duties.

Privacy Protection Policy & Procedure

Label	Description	Examples	Rules
		Student or employer payment details LLND assessment records Student welfare records Student visa information Overseas student contact details	Secure storage, transmission, and disposal required. Classification label must be applied where practical and appropriate.
Critical	Information vital for the ongoing operations, continuity, and stability of the business. Its loss or compromise could severely impact operations.	Business continuity plans Critical infrastructure documentation Insurance records Administrator security credentials Business continuity and disaster recovery records Cybersecurity credentials Server access credentials	Secure storage with regular backups. Limited access to authorised personnel. Regular integrity checks/audits. Classification label must be applied where practical and appropriate.
Regulatory	Information required by law, regulations, industry standards, or compliance frameworks. Disclosure, handling, or storage governed externally.	Records that show compliance with standards Financial viability information Work health and safety records AVETMISS records PRISMS reporting records	Comply fully with relevant regulations. Regular audits and monitoring. Clear recordkeeping and accountability required.

Privacy Protection Policy & Procedure

Label	Description	Examples	Rules
		CRICOS compliance records Trainer matrix and credential records	

3.14 Privacy of Overseas Students (CRICOS Requirements)

Princeton International College ensures that the personal information of overseas students is collected, used, stored, accessed and disclosed in accordance with the ESOS Act 2000, National Code of Practice for Providers of Education and Training to Overseas Students 2018, Privacy Act 1988 and Australian Privacy Principles (APPs).

Princeton International College recognises the importance of maintaining the privacy, confidentiality and security of overseas student information throughout the student lifecycle, including pre-enrolment, enrolment, training and assessment, student support, course progression, wellbeing support, PRISMS reporting and course completion processes.

The College will ensure that:

- personal information is collected only where necessary for enrolment, student administration, training and assessment, learner support, wellbeing support, regulatory reporting, visa compliance obligations or other lawful operational purposes
- overseas students are informed about the collection, use and disclosure of their personal information prior to or at the time of enrolment, including through the Student Handbook, enrolment documentation, written agreements and privacy notifications
- personal information is disclosed only where authorised under legislation, required for regulatory reporting purposes, required under the ESOS framework, or with the student's consent
- information required for regulatory reporting, including PRISMS and AVETMISS reporting, is managed accurately and securely
- student records and personal information are maintained confidentially at all times and access is restricted to authorised personnel only

Privacy Protection Policy & Procedure

- personal information is protected from misuse, interference, loss, unauthorised access, modification or disclosure through appropriate physical, digital and operational security controls
- personal information is not disclosed to overseas recipients unless authorised by law, required for operational purposes with appropriate controls, or with the student's consent
- student welfare, wellbeing, support and engagement information is handled sensitively and confidentially in accordance with legislative and organisational requirements
- overseas students may request access to or correction of their personal information in accordance with Princeton International College policies, procedures and applicable privacy legislation

3.15 Data Breach Response

In the event of a suspected or actual data breach, Princeton International College will respond promptly in accordance with the Privacy Act 1988 and the Notifiable Data Breaches scheme. This includes taking reasonable steps to contain the breach, assess the nature and extent of the breach, mitigate the risk of harm, notify affected individuals where required, notify the Office of the Australian Information Commissioner (OAIC) where an eligible data breach has occurred, and implement corrective action to prevent recurrence.

4. Procedure

Princeton International College implements privacy, confidentiality, records management and information security procedures across all operational areas to ensure personal and sensitive information is managed securely, lawfully and consistently throughout the student and staff lifecycle.

Privacy and information handling procedures are integrated throughout Princeton International College's governance, student administration, training, assessment, student support, workforce management and compliance management systems.

The following Princeton International College policies, procedures and operational processes support the implementation of this policy:



Privacy Protection Policy & Procedure

- Student enrolment, pre-enrolment assessment, LLND assessment, collection of personal information and written agreement processes are managed in accordance with the:
 - Pre-Enrolment Policy and Procedure
 - Formalisation of Enrolment and Written Agreement Policy and Procedure
 - LLND Policy and Procedure
- Student support, wellbeing, welfare support, learner intervention, student engagement monitoring and support record management processes are managed in accordance with the:
 - Student Support and Wellbeing Policy and Procedure
 - VET Student Engagement and Non-Attendance Policy and Procedure
 - Monitoring International Student VET Course Progress Policy and Procedure
 - ELICOS Attendance Monitoring Policy and Procedure
- Student complaints, appeals, behaviour management and misconduct-related information handling processes are managed in accordance with the:
 - Complaints Handling Policy and Procedure
 - Appeals Handling Policy and Procedure
 - Student Behaviour and Misconduct Policy and Procedure
- Student enrolment variations, transfers, deferment, suspension, cancellation, refunds and PRISMS-related information management processes are managed in accordance with the:
 - Deferring, Suspending or Cancelling Student Enrolment Policy and Procedure
 - Transfer Between Registered Providers Policy and Procedure
 - Extending Course Duration Policy and Procedure
 - Fees and Refund Policy and Procedure

Privacy Protection Policy & Procedure

- Student record retention, issuing of certification documentation, AVETMISS reporting, PRISMS reporting and regulatory record management processes are managed in accordance with the:
 - Records Management Policy and Procedure
 - Qualifications & Statement of Attainment Policy & Procedure
 - Reporting Obligations and Regulatory Compliance procedures
- Workforce recruitment, staff induction, trainer credential management, staff performance management and personnel record handling processes are managed in accordance with the:
 - Workforce Planning, Recruitment and Induction procedures
 - Trainer and Assessor Credential Requirements Policy and Procedure
 - Performance Management procedures

All staff are responsible for ensuring that personal and sensitive information accessed during operational activities is handled confidentially and in accordance with Princeton International College's privacy, information security and records management requirements.

5. Roles and Responsibilities

Princeton International College ensures that responsibilities relating to privacy management, information security, confidentiality and records management are clearly defined and implemented across all operational areas.

Position	Responsibilities
Chief Executive Officer (CEO)	Maintains overall responsibility for governance oversight, privacy compliance, information governance, records management, information security and regulatory compliance obligations across Princeton International College. Oversees privacy risks, data breach management, regulatory reporting, information security controls and continuous improvement activities relating to privacy and information management.

Privacy Protection Policy & Procedure

Position	Responsibilities
Administration Officer	Assists with the management of student records, document handling, secure information storage, record retention, archiving and maintenance of authorised institutional systems including Wisenet and approved cloud-based systems. Supports implementation of privacy, confidentiality and records management practices across operational areas.
Student Support Officer	Assists with maintaining confidentiality of student wellbeing, welfare, engagement and support-related information. Ensures student information is handled appropriately during student support, welfare, intervention and engagement activities and escalates privacy concerns where required.
Training Manager	Oversees secure management of learner records, assessment records, course progress records, validation records and academic information relating to VET operations. Ensures access to academic and assessment information is restricted to authorised personnel only.
ELICOS Coordinator	Oversees secure management of ELICOS attendance records, academic records, learner support information and student engagement records relating to ELICOS operations. Ensures information is managed confidentially and in accordance with operational and regulatory requirements.
All Staff	Must maintain confidentiality, protect personal and sensitive information, comply with privacy and information security requirements, follow authorised information handling procedures and immediately report any suspected privacy breach, information security risk or unauthorised disclosure of information.

6. Records Management

Princeton International College maintains accurate, secure and accessible records relating to personal information, student information, staff information, privacy management, information security activities, consent records, complaints, appeals, regulatory reporting and operational activities.

Privacy Protection Policy & Procedure

Records are maintained within authorised institutional systems, including Wisenet, secure cloud-based platforms and approved digital storage systems, with access restricted to authorised personnel only.

Physical and electronic records containing personal or sensitive information are managed, retained, archived and securely disposed of in accordance with legislative requirements, operational requirements and Princeton International College's Records Management Policy and Procedure.

Operational implementation of privacy, confidentiality and information security controls is supported by authorised administrative and academic staff across relevant operational areas.

7. Continuous Improvement

Princeton International College reviews privacy management practices, information security controls, records management processes, digital security measures and information handling practices as part of its continuous improvement and governance framework.

Privacy incidents, identified risks, complaints, audit findings, data management issues, system vulnerabilities and regulatory updates are monitored to identify opportunities for improvement.

Improvement actions, corrective actions and identified privacy or information security risks are recorded within the Continuous Improvement Register and monitored through management and governance processes under the oversight of the CEO.