GBC Privacy Policy and Procedure

1. Purpose

The purpose of this Policy and Procedure is to ensure the confidentiality, security and proper handling of students', staff and stakeholder personal data ensuring the protection of individual privacy.

These measures align with the Privacy Act 1988, incorporating the Australian Privacy Principles (APPs) and the amendments made by the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

2. Rationale

The Privacy Policy and Procedure is a critical component of George Brown College's (GBC) governance and compliance framework. It ensures that the collection, storage, use, and disclosure of personal information complies with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Student Identifiers Act 2014, and relevant VET sector legislation including the National Vocational Education and Training Regulator Act 2011.

GBC is entrusted with the personal and sensitive information of students, staff, contractors, and stakeholders. The integrity and security of this information is fundamental to maintaining the trust of these individuals and meeting our statutory obligations. The consequences of mishandling personal information include not only reputational damage and legal liability but also potential disruption to operations and student outcomes.

This Policy and Procedure provides a clear, structured approach to privacy protection by setting out guiding principles, responsibilities, and processes for the lawful and secure management of personal information. It reflects a commitment to best practice in data protection, risk management, and digital security, ensuring that information is handled with the utmost care and in accordance with evolving regulatory expectations under the Standards for RTOs 2025.

By embedding privacy protections in daily operations, this policy contributes to the ethical and compliant delivery of training services and supports our broader objectives of quality assurance, transparency, and student-centred practice.

3. Policy

GBC is committed to protecting the privacy and security of personal information and to upholding the rights of individuals. This Privacy Policy and Procedure ensures that personal

information is handled lawfully, securely, and transparently in accordance with relevant legislation and regulatory standards.

GBC manages all personal information in compliance with the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs), and the Privacy Amendment (Enhancing Privacy Protection) Act 2012. This policy also aligns with the Standards for Registered Training Organisations 2025, the National Vocational Education and Training Regulator Act 2011 (Cth) (NVETR Act), the Student Identifiers Act 2014, and the Data Provision Requirements 2020.

In accordance with the NVETR Act, GBC is obligated to disclose personal information collected from students to the National VET Data Collection, managed by the National Centre for Vocational Education Research Ltd (NCVER), and, where applicable, to the relevant state or territory training authority.

GBC also complies with the Data Provision Requirements 2020, which mandate the collection, verification, and submission of accurate AVETMISS data to NCVER for national VET policy and planning purposes. All data collected under these provisions is managed securely and in alignment with the Privacy Act 1988 and the APPs.

All students undertaking nationally recognised training are required to have a Unique Student Identifier (USI). Students must provide their USI at enrolment, or GBC may apply for a USI on their behalf. The Student Identifiers Act 2014 authorises the Australian Government's Student Identifiers Registrar to collect personal information to create and manage USIs.

When applying for a USI on a student's behalf, GBC must collect and provide the following personal information to the Registrar:

- Name (including given name(s), middle name(s), and family name)
- Date of birth
- City or town of birth
- Country of birth
- Gender
- Contact details

Where a student does not provide the required information, the USI Registrar will be unable to issue a USI, and GBC will not be able to issue a qualification or statement of attainment.

For CRICOS students, GBC complies with the requirements of the Education Services for Overseas Students Act 2000 (ESOS Act) and the National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code). GBC informs overseas students that their personal information may be made available to the Australian Government and designated authorities including the Tuition Protection Service (TPS), the Department of Education, the Department of Home Affairs, and other agencies authorised by law. This information may include details relating to course progress, visa status, and payment records.

4. Responsibility

Director/designated Privacy Officer is responsible for implementing and monitoring the Privacy Policy and Procedures and for addressing any queries or concerns about privacy matters.
CEO, supported by an external IT provider, oversees cybersecurity compliance.

5. legislative Requirements

GBC must act in accord with the requirements of the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs) and the Privacy Amendment (Enhancing Privacy Protection) Act 2012.

Data Provision Requirements 2020 (legislative instrument made under section 187 of the National Vocational Education and Training Regulator Act 2011).

Education Services for Overseas Students Act 2000 (ESOS Act), National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code).

It must also comply with the Standards for Registered Training Organisations (RTOs) 2025 - Standard 4.4 (2) (c) - *it has mechanisms in place to lawfully collect and analyse data including any feedback received from VET students, staff, industry, VET regulators, State and Territory training authorities and employers of current or former VET students*.

6. Definitions

Personal Information defined under the Privacy Act 1988 (Cth) refers to any information or opinion about an individual, or that may reasonably identify an individual.
Privacy Act 1988 refers to an Australian law which regulates the handling of personal information about individuals.
Australian Privacy Principles (APPs) are contained in the Privacy Act 1988 and outline the handling, use and management of personal information.
Consent as per the Australian Privacy Principles ((s 6(1)) refers to 'express consent or implied consent'. The four key elements of consent include the individual being adequately informed before giving consent, the individual giving consent voluntarily, the consent is current and specific, and the individual has the capacity to understand and communicate their consent.

7. Scope

This policy applies to all employees, students, contractors, and other individuals associated with GBC who are involved in the collection, use, and disclosure of personal information.

This policy applies to all students enrolled with GBC, including both domestic students and international students studying in Australia on a student visa (CRICOS students). It is intended

to ensure consistent application of the RTO's responsibilities under the Standards for RTOs 2025 and, where applicable, the Education Services for Overseas Students Act 2000 and the National Code of Practice for Providers of Education and Training to Overseas Students 2018. Where obligations differ for CRICOS students, specific provisions are identified within the policy and procedure.

8. Procedure

GBC ensures the lawful, fair, and secure handling of personal information throughout its lifecycle. Personal information is collected directly from students, staff, or stakeholders through enrolment forms, consent forms, applications, and correspondence. Information collected is limited to what is reasonably necessary for training delivery, compliance, reporting, and student support. GBC notifies individuals at or before the time of collection through the Student Handbook and privacy statements and seeks informed consent where required. Once collected, this information is used to support training delivery, reporting, and compliance functions in accordance with privacy laws.

Once collected, personal information is used for enrolment processing, student management, support services, training delivery, compliance with reporting requirements, and issuing qualifications. Use and disclosure are limited to the primary purpose of collection or a directly related secondary purpose where consent is provided or legally required. Disclosure may be made to NCVER, the USI Registrar, government agencies, and authorised third parties for regulatory, statistical, and funding purposes.

All personal information is stored securely, either digitally within password-protected systems or physically in locked storage. GBC uses encryption, access controls, and antivirus software to protect digital data. Multi-factor authentication (MFA) and secure backups are implemented to minimise cybersecurity risks. Information classification labels guide staff on handling sensitive data, such as those marked Confidential or Restricted.

Students have the right to request access to or correction of their information. Requests are responded to within 10 business days. If personal information becomes unnecessary for any purpose, it is securely destroyed or de-identified. High-risk personal information (e.g. passport, licence) is not retained after use and is instead logged via a verification record.

In accordance with Standard 4.4(2)(c) of the Standards for RTOs 2025, GBC collects feedback from students, staff, industry, regulators, training authorities, and employers of current or former students to inform continuous improvement. This feedback may include personal or sensitive information. GBC ensures that all such feedback is handled in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

Feedback is stored securely, access is limited to authorised personnel, and it is only used for the purpose for which it was collected, such as quality assurance and reporting. Identifiable data is de-identified where possible, and feedback mechanisms are subject to regular review as part of GBC's self-assurance practices.

If GBC receives unsolicited personal information it is assessed and, if not required, securely destroyed. Any marketing communication complies with APP 7 and allows individuals to opt-out.

Privacy-related complaints can be submitted to the Privacy Officer. Complaints are handled under the Complaints and Appeals Policy and may be escalated to the Office of the Australian Information Commissioner (OAIC) if unresolved. Privacy compliance is reviewed regularly by the CEO with issues addressed through the Continuous Improvement Register.

Procedure Table

Step	Action	Responsible	Timeframe	Record/Reference
1	Collect personal information via forms, systems, or correspondence	Admin/Trainer	At time of enrolment or service	Enrolment Form, USI record
2	Notify individuals and obtain consent	Admin	Before or at time of collection	Privacy Statement, Student Handbook
3	Use and disclose information as required (including AVETMISS-compliant data submissions under the Data Provision Requirements 2020	Admin/Compliance	As needed	Student File, AVETMISS data
4	Store and protect personal information securely	Admin/IT	Ongoing	Student Management System, Secure Cabinet
5	Log verification of high-risk documents (do not retain)	Admin	At verification	Verification Log
6	Destroy or de-identify unneeded personal data	Admin	As soon as no longer required	Destruction Log
7	Respond to access or correction requests	Admin	Within 10 working days	Student File, Correspondence Log
8	Handle privacy complaints	Privacy Officer/Director	As received	Complaints Register
9	Conduct regular compliance monitoring	Director	Monthly	Continuous Improvement Register

9. Policy Implementation

This policy will be made available to all staff members and stakeholders through the internal communication channels, the website and in the Student Handbook.

All staff receive annual cybersecurity training including identifying phishing, secure password handling, and digital confidentiality.

10. Review

Privacy compliance issues are a standing agenda item at monthly management meetings. Feedback from staff and students is collated, reviewed, and addressed via the Continuous Improvement Register.

This Policy and Procedure will undergo an annual review, or sooner if required, to ensure it remains relevant and effective in guiding the operations and strategies or as needed to reflect any changes in the regulatory environment or operational practices.

Feedback will be collated and analysed and discussed at the monthly management meetings, for noting or action with any necessary changes documented in a Continuous Improvement Form and in the Continuous Improvement Register.

Document Control

Version number:	V1	Approved by:	Preeti Singh
Approval date:	1/07/2025	Review date:	02/07/2026
Standards: 4.4 (2) (c)			
Legislation: Privacy Act 1988, Privacy Amendment (Enhancing Privacy Protection) Act 2012, Student Identifiers Act 2014, National Vocational Education and Training Regulator Act 2011, Data Provision Requirements 2020, Education Services for Overseas Students Act 2000 (ESOS Act), National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code)			

Version #	**Changes**	**Approval By**	**Approval Date**
1.0	**Original Version**	**PEO**	**1/07/2025**

Associated Policies

This policy must be read in conjunction with the following policies:

- Enrolment Policy and Procedure
- Complaints and Appeals Policy and Procedure
- Record Retention Policy
- Student Support and Wellbeing Policy
- Behaviour Misconduct Policy
- Workforce Planning and Recruitment Policy