Policy

Privacy and Confidentiality

Date of approval	26 March 2025	**Approved by**	Senior Executive Team (SET)
Date of effect	26 March 2025	**Review date**	31 March 2028
Responsible Owner	Deputy Chief Executive Officer - Operations	**Version**	v1 2026
Functional Manager	Director Corporate Governance and Risk Office (CGRO)		

1. Outline and Scope

1.1 The Batchelor Institute of Indigenous Tertiary Education (the Institute) is a Public Sector organisation for the purposes of the Northern Territory *Information Act 2002*. The Act provides for:

- Access to personal information held by the Institute in conjunction with each individual's right to privacy;
- An ability for individuals to correct information held by the institute;
- An individual to expect the Institute to responsibly collect and handle their personal information; and
- The Institute to appropriately manage and archive their personal information.

The Institute is subject to the *Information Act 2002* as stated above. It is also subject to the relevant provisions of the Commonwealth *Privacy Act 1988* through the operation of Section 7 of the Privacy Act.

1.2 The Institute is committed to protecting the privacy of all stakeholders of the Institute for which it collects, stores or reports personal information.

1.3 **Scope.**

1.3.1 This policy relates to the privacy of personal information and applies to all areas of the Institute and to all staff and students.

1.3.2 All staff and students of the Institute and others who are responsible for the collection, handling, storage, disposal and access to personal and confidential information must be aware of their responsibilities under the *Information Act 2002*. This policy also applies where such information may be incidentally collected, stored or reported as part of or outside their normal duties pertaining to the Institute.

1.3.3 As a Registered Training Organisation (RTO) and Higher Education Provider (HEP) the Institute also has obligations under Commonwealth legislation and regulatory requirements in regard to student and staff information. This includes government-related identifiers and personal information the Institute collects and holds regarding student assistance, provided by the Commonwealth (which is an obligation under Section 19-60 of the *Higher Education Support Act 2003* and *the VET Student Loans Act 2016*).

2. Summary

2.1 This policy provides guidance and principles for the protection of personal privacy and information as required by the Information Act 2002 and other legislative instruments.

2.2 This policy while complying with relevant legislation aims to protect students, staff and other relevant stakeholders of the Institute from unauthorised or unwarranted collection or disclosure of their personal information. This includes relevant information relating to Indigenous Australian Sacred Sites, Traditions or confidential cultural information.

3. Policy

Collection of Personal Information

3.1 The Institute will only collect personal information that is necessary for its functions or activities.

3.2 The Institute will only collect personal information in a lawful, fair and not unreasonably intrusive way.

3.3 When personal information is collected from an individual, the Institute will take reasonable steps to ensure that the individual is:

a. aware of the Institute's identity and its contact information;

b. able to have access to the information;

c. aware of the purpose for which the information is collected;

d. aware of the persons or bodies, or classes of persons or bodies, to which the Institute usually discloses personal information;

e. aware of any law that requires the collection of the information; and

f. aware of any consequences for the individual if they do not provide all or part of the information.

3.4 If it is reasonable and practical to do so, the Institute will only collect personal information about an individual from that individual. If the Institute collects personal information about an individual from another person, it will take reasonable steps to ensure the individual is or has been made aware of the matters listed above unless making the individual aware of these matters would pose a serious threat to the life or health of a person.

Use and Disclosure

3.5 The Institute may use and disclose personal information only in the following instances:

a. The use or disclosure is related or directly related to the purpose for collecting it and the individual would reasonably expect the Institute to use or disclose it for that purpose;

b. with the individual's consent, including for research purposes approved in line with the human research ethics process;

c. where the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest and the following apply:

   i. the research will not be published in identifiable form;

   ii. the individual's consent cannot be reasonably obtained;

   iii. the recipient of the information will not disclose the personal information;

   iv. if the information is health information, the use or disclosure is in accordance with guidelines issued by the Information Commissioner under section 86(1)(a)(iv) of the Information Act 2002; and

   v. in the case of human research, when appropriate ethics clearance has been given.

d. to lessen or prevent a serious and imminent threat to a person's life, health or safety, or of harm to or exploitation of a child, or serious threat to public health or safety;

e. when required in the investigation or reporting of unlawful activity, or assisting a law enforcement agency;

f. where the use or disclosure is required or authorised by law; or

g. in connection with the performance of the functions of the Australian Security Intelligence Office (ASIO) or Australian Secret Intelligence Service (ASIS) where authorised in writing.

Trans-border Data Flows

3.6 The Institute will not transfer personal information about an individual to a person (other than the individual) outside the Northern Territory unless:

a. the transfer is required or authorised under a law of the Northern Territory or the Commonwealth; or

b. the Institute reasonably believes that the person receiving the information is subject to a law, or a contract or other legally binding arrangement, that requires the person to comply with principles for handling the information that are substantially similar to the Information Privacy Principles and Australian Privacy Principles; or

c. the individual consents to the transfer; or

d. the transfer is necessary for the performance of a contract between the organisation and the individual or for the implementation of pre-contractual measures taken in response to the individual's request; or

e. the transfer is necessary for the performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the individual; or

f. all of the following apply:

   i. the transfer is for the benefit of the individual;

   ii. it is impracticable to obtain the consent of the individual to the transfer;

   iii. it is likely that the individual would consent to the transfer; or

   iv. the organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the person to whom it is transferred, in a manner that is inconsistent with the Information Privacy Principles.

3.7 The Institute will ensure that any contracts with third parties where personal information may be transferred, contain privacy clauses requiring compliance with the [Information Act 2002] and the Information Privacy Principles and the

Privacy Act 1988 where it pertains to this policy.

Data Quality

3.8 The Institute will take all reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date.

Data Breaches

3.9 The Notifiable Data Breach Scheme, as detailed in the Privacy Act 1988 requires regulated entities to notify affected individuals and the Australian Information Commissioner about the occurrence of eligible data breaches. The Institute is only subject to the requirements of the Notifiable Data Breaches Scheme, where it relates to:

a. Tax File Number (TFN) information;

b. Government-related identifiers; and

c. Personal information the Institute collects and holds regarding student assistance, provided by the Commonwealth (which is an obligation under Section 19-60 of the *Higher Education Support Act 2003* and the *VET Student Loans Act 2016*.

3.10 All suspected data breaches must be referred to the Institute's Privacy Officer at privacy.officer@batchelor.edu.au for actioning and reporting as deemed appropriate.

Data Security

3.11 The Institute will take all reasonable steps to protect all personal information it holds from misuse, loss, unauthorised access, modification or disclosure.

3.12 Security, integrity and accuracy of information is governed by the Institute's Information and Communication Technology and Cyber-Security policies and procedures.

3.13 The Institute will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose in accordance with the retention and disposal schedules.

Openness

3.14 The Institute publishes a Privacy Statement which describes how it manages personal information. The Privacy Statement is available at the bottom of the Institutes website.

Privacy and Confidentiality Obligations

3.15 Staff, students, researchers, contractors and any other third party who collect use or disclose personal information on behalf of the Institute have a responsibility to act consistent with the Information Privacy Principles (IPP) outlined in *Information Act 2002* and Australian Privacy Principles (APP) outlined in the *Privacy Act 1988*, and to take appropriate measures to avoid a breach of confidence.

3.16 Under the *Higher Education Support Act 2003,* it is an offence (punishable by fine or imprisonment), if a staff member of the Institute discloses, copies or records personal information otherwise than in the course of official employment, or causes unauthorised access to or modification of personal information held by the Institute.

3.17 At any time during and after employment with the Institute, a staff member must not use, divulge, copy or communicate any confidential information to any person without the Institute's consent, regardless of whether the other person is a staff member of the Institute or not, except as required in the ordinary performance of the staff members' duties.

3.18 Unauthorised access to personal information must be reported to the Institute's Privacy Officer and, where relevant, to the responsible owner of the information system concerned. Failure to comply with this Policy may necessitate disciplinary action.

3.19 Institute matters relating to individuals or non-public information must not be discussed, except where directly related to the staff member's role, as this may constitute a breach of confidence and therefore misconduct.

Information and Communication Technologies Facilities

3.20 Users of the Institute's Information and Communication Technologies (ICT) facilities or systems are reminded that anything that is written or recorded is potentially subject to subpoena or Freedom of Information requests or other authorised access. Inappropriate use of the Institute's ICT facilities or systems may be subject to disciplinary action.

Access and Correction

3.21 On the request of an individual, the Institute will provide access to their personal information, except to the extent that:

a. providing access would pose a serious threat to the life or health of the individual or another individual; or

b. providing access would prejudice measures for the protection of the health or safety of the public; or

c. providing access would unreasonably interfere with the privacy of another individual; or

d. the request for access is frivolous or vexatious; or

e. the information relates to existing or anticipated legal proceedings between the Institute and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

f. providing access would reveal the intentions of the Institute in relation to negotiations with the individual in such a way that would prejudice the negotiations; or

g. providing access would be unlawful; or

h. denying access is required or authorised by law; or

i. providing access would be likely to prejudice an investigation of possible unlawful activity; or

j. providing access would be likely to prejudice one or more of the following by or on behalf of a law enforcement agency:

    i. preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;

    ii. enforcing a law relating to the confiscation of proceeds of crime;

    iii. protecting public revenue;

iv. preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;

v. preparing for or conducting proceedings in a court or tribunal or implementing the orders of a court or tribunal; or

vi. providing access would prejudice:

vii. the security or defence of the Commonwealth or a State or Territory of the Commonwealth; or

viii. the maintenance of law and order in the Territory.

3.22 However, where providing access would reveal evaluative information generated within the Institute in connection with a commercially sensitive decision-making process, the Institute may give the individual an explanation for the commercially sensitive decision rather than access to the decision.

3.23 If the Institute holds personal information about an individual and the individual establishes that the information is not accurate, complete or up to date, the Institute will take reasonable steps to correct the information so that it is accurate, complete and up to date.

3.24 If an individual and the Institute disagree about whether personal information about the individual held by the Institute is accurate, complete or up to date; and

a. The individual requests the Institute to include with the information a statement to the effect that, in the individual's opinion, the information is inaccurate, incomplete or out of date;

b. The Institute will take reasonable steps to comply with that request.

3.25 The Institute will provide reasons for refusing to provide access to or correct personal information.

3.26 If an individual requests the Institute for access to, or to correct personal information held by the Institute, the Institute will, within a reasonable time:

a. Provide access or reasons for refusing access; or

b. Make the correction or provide reasons for refusing to make it; or

c. Provide reasons for the delay in responding to the request;

3.27 If the Institute charges a fee for providing access to personal information, the fee will not be excessive. Access and amendment requests should be directed to the Institute’s Privacy Officer.

Notification of correction to third parties

3.28 If the Institute corrects personal information that the Institute previously disclosed to another entity, and the individual requests the Institute to notify the other entity of the correction, the Institute will take such steps as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Identifiers

3.29 The Institute will not assign unique identifiers to individuals unless it is necessary to enable the organisation to perform its functions efficiently.

3.30 The Institute will not ask individuals to provide a unique identifier in order to obtain a service unless its provision is required or authorised by law or is in connection with the purpose for which the unique identifier was assigned or for a directly related purpose. For example, provision of a Unique Student identifier (USI).

Anonymity

3.31 The Institute must give an individual entering transactions with the organisation the option of not identifying himself or herself unless it is required by law or it is not practicable that the individual is not identified.

Sensitive Information

3.32 The Institute will not collect sensitive information about an individual unless:

a. the individual consents to the collection; or

b. the Institute is authorised or required by law to collect the information; or

c. the individual is:

   i. physically or legally incapable of giving consent to the collection; or

   ii. physically unable to communicate his or her consent to the collection; and

   iii. collecting the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another individual;

d. collecting the information is necessary to establish, exercise or defend a legal or equitable claim.

3.33 However, the Institute may collect sensitive information about an individual if:

a. the collection:

   i. is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

   ii. is of information relating to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services; and

b. there is no other reasonably practicable alternative to collecting the information for that purpose; and

c. it is impracticable for the organisation to seek the individual's consent to the collection.

4. Acronyms & Terms

Acronym/Term	***Definition/Description***
Personal Information	Personal Information means any information or opinion about an individual whose identity is apparent or can reasonably be ascertained. It may include name, address, date of birth, staff or student identification number, financial/pay details. This includes personal information pertaining to current and former students, current and former staff, and associates of the Institute. Personal information does not include information about an individual that is contained within publicly available publications.

Acronym/Term	Definition/Description
Sensitive Information	As defined in the *Information Act 2002* (NT). However, among other things sensitive information may include information about racial or ethnic origin, health, political opinions, religious or philosophical beliefs, criminal record, or membership of a professional or trade association.
Staff	means individuals who are employed or engaged, by or for the Institute, and whether for reward or on a voluntary basis. It includes adjuncts, volunteers, contractors and individuals employed by contractors within or outside the Northern Territory. Contractors do not include trade contractors such as those employed by facilities or campus operations.

5. Supporting Batchelor Institute documents

- Batchelor Institute Union Enterprise Agreement,
- Council Members Code of Conduct,
- Staff Code of Conduct,
- Student Code of Conduct,
- Information and Communications Technology Policy,
- Student Records Retention Schedule,
- Application to access information,
- Application to correct information,
- Application for internal review,
- Application to waive or reduce fees.

6. Related documents

- *Information Act 2002* (NT),
- *Information Regulations 2003* (NT),
- *Privacy Act 1988* (Cth),
- *Higher Education Support Act 2003,*
- *National Vocational Education and Training Regulator Act 2011,*
- National VET Provider Collection Data Requirement Policy,
- *Student Identifiers Act 2014,*
- *Higher Education Standards Framework (Threshold Standards) 2021,*
- Standards for Registered Training Organisations (RTOs) 2025,
- *Fair Work Act 2009,*
- *Independent Commissioner Against Corruption Act 2017.*

7. Modification history

Date	*Version*	*Sections modified*	*Authority*	*Details*
April 2015	1	Complete revise of previous policy	EMG	New Policy
November 2016	2016 - 1	Titles, sect 4	Senior Policy Officer	Change in titles due to organisational changes
March 2025	v1 2025	All sections	SET	Complete rewrite
February 2026	v1 2026		Director CGRO	Amend Functional Manager title. Change to Director CGRO.

8. Non-Compliance and Issues

8.1 Non-compliance with this policy is considered a breach of the applicable code of conduct and is treated seriously by the Institute.

8.2 Any issues regarding the treatment of personal or sensitive information should in the first instance be addressed to the Institute's Privacy Officer at: privacy.officer@batchelor.edu.au

8.3 In some circumstances complaints may also be directed to the Northern Territory Information Commissioner. Information regarding the Information Commissioner can be obtained at Home | The Office of the Information Commissioner Northern Territory.

8.3 All staff members have a responsibility to raise any suspicion, allegation or report of the categories of improper conduct in accordance with the Fraud and Corruption Control Policy and the Whistleblower Reporting (Improper Conduct) Procedure and Guideline.

9. Feedback

If you have any comments or feedback about this policy, please contact the Privacy Officer at privacy.officer@batchelor.edu.au .