

Policy Owner: College Director and Principal
Keywords: Personal, Sensitive and Health Information, Privacy
Policy Code: QBIP0002

[Intent](#)
[Organisational Scope](#)
[Definitions](#)
[Policy Content](#)
[Accountabilities and Responsibilities](#)
[Related Documents](#)
[Contact Information](#)
[Approval History](#)

1. INTENT

- 1.1 This Policy outlines the way Personal, Sensitive and Health information is collected, shared and used by Edith Cowan College.
- 1.2 This Policy is designed to:
- a) substantially reflect the [Australian Privacy Principles](#), although Edith Cowan College is not bound by the provision;
 - b) comply with the [Privacy Act 1988](#); and
 - c) meets the requirements of the Australian Government's [Notifiable Data Breach \(NDB\) Scheme](#).
- 1.3 As a Joint Venture College, ECC shares some Personal, Sensitive and Health information with its university partner, Edith Cowan University and its Pathway education partner, Navitas Pty Ltd to meet legal and regulatory requirements and to fulfill ECC's contractual agreements with Students. This Policy was written to complement the privacy policies of both partners (see the [Navitas Privacy Policy](#) and [ECU Privacy Policy](#)).

2. ORGANISATIONAL SCOPE

- 2.1 This Policy applies to all Staff and Students at ECC.

3. DEFINITIONS:

- 3.1 The [Glossary of Policy Terms](#) applies to this Policy.

4. POLICY CONTENT:

General Principles

- 4.1 ECC will collect, use and disclose Personal, Sensitive and Health Information in a manner that is consistent with this Policy.
- 4.2 Whilst ECC will use reasonable endeavours to ensure its collection, use and disclosure is broadly consistent with the Australian Privacy Principles (APP) as defined in the [Privacy Act 1988 \(Cth\)](#), the College is only bound by the [Privacy Act 1988 \(Cth\)](#) in the following circumstances:
- the collection, use and disclosure of information obtained for the purposes prescribed by the [Higher Education Support Act 2003 \(Cth\)](#);
 - the collection, use, disclosure, and management of data concerning tax file number information of individuals; and
 - where it has agreed to be contractually bound.

Privacy by Design

- 4.3 ECC follows a Privacy by Design approach to the management of Personal, Sensitive and Health Information:
- proactive/preventative:** reasonable steps will be taken to protect the information it captures and holds from misuse, loss and unauthorised access, modification or disclosure;
 - privacy by default:** Staff will ensure that information is automatically protected in all IT systems or business practices that will be introduced or amended by a project, so that no added action is needed by any individual;
 - embedded into design:** privacy measures including data minimisation will be included within the scope and quality requirements for all projects, so that they are fully integrated components of the system;
 - positive-sum not zero-sum:** Privacy by Design will be fully implemented within all system and process designs, factoring in both privacy and security;
 - end-to-end lifecycle security:** systems and processes will be aligned to relevant data lifecycle security and that data is stored, retained and destroyed when it is no longer required;
 - maintain viability and transparency:** all stakeholders are assured that personal information operate according to relevant compliance requirements changes are fully tested and are subject to independent verification; and
 - respect user privacy:** individuals' privacy will be underpinned by privacy defaults, notices and user-centric options.

Collection of Personal Information

- 4.4 when collecting solicited Personal Information, ECC will only collect Personal Information:
- a) for lawful purposes and when reasonably necessary for, or related to, the College's functions, services or activities; and
 - b) from the individual it relates to, unless;
 - i. the individual has consented otherwise;
 - ii. it is required or authorized by Australian law or a court or tribunal order; or
 - iii. it is unreasonable or impracticable to do so.
- 4.5 Where ECC receives unsolicited Personal Information, it will determine whether processing such information is reasonably necessary for, or directly related to, the College's functions or activities, and whether ECC could have collected the Personal Information if the college had solicited the information. If so, the provisions of this Policy will apply to the use, disclosure and management of that information. Otherwise, where lawful and reasonable to do so, unsolicited information will be destroyed or de-identified.
- 4.6 ECC will only collect Sensitive Information where either:
- a) a person consents to the information being collected and the information is reasonably necessary for, or directly related to, the College's functions or activities;
 - b) it is required or authorized under an Australian law or a court or tribunal order; or
 - c) a Permitted General Situation or Permitted Health Situation exists; or
 - d) the information relates to ECC functions or activities, and the information relates solely to College Staff or Students, or to individuals who have regular contact with ECC in connection with its functions or activities.
- 4.7 At or before the time the College collects Personal Information about an individual, or if that is not practicable, as soon as possible thereafter, ECC will take reasonable steps to notify the individual of those matters set out below, or otherwise ensure that the individual is aware of the matters set out below, as may be reasonable in the circumstances:
- a) the College's contact details;
 - b) where the College has collected Personal Information from someone other than the individual, or the individual may not be aware that the College has collected the Personal Information, the fact that the Personal Information has been collected and the circumstances around its collection;
 - c) the purpose for collecting the Personal Information;
 - d) the main consequences (if any) for the individual if ECC does not collect some or all of the Personal Information; and

- e) that the individual's Personal Information will otherwise be managed in accordance with this Policy, including the individual's rights to access to correct information, and access ECCs complaints processes.

Protection and De-Identification or Destruction of Personal Information

4.8 ECC will take reasonable steps to:

- a) protect a person's Personal Information, including from misuse, interference, loss and from unauthorized access, modification and disclosure; and
- b) de-identify or destroy Personal Information about an individual where the:
 - i. College no longer needs the information for a purpose for which the information may be used or disclosed by the entity under this Policy;
 - ii. information is not contained in a Commonwealth record; and
 - iii. ECC is not required by or under an Australian law, or a court or tribunal order, to retain the information.

Use and Disclosure of Personal Information

4.9 Use and disclosure of Personal Information by ECC should be reasonably necessary for, or related to, the College's functions, services, and activities. Subject to Clauses 4.12 and 4.13 relating to Sensitive Information, ECC will not use or disclose Personal Information unless:

- a) the person whom the information is about has expressly, or by inference, consented to its use or disclosure;
- b) it is reasonable to expect that ECC would use or disclose the information in the ordinary course of its functions or activities, including to meet its compliance and reporting obligations, and the improvement of its products and services;
- c) it is required or authorised by Australian law or a court or tribunal order;
- d) it is reasonable in the circumstances to disclose the information to entities or bodies such as government agencies, statutory boards, law enforcement agencies, accreditation or registration bodies, independent oversight bodies, regulators, mediators, or conciliators, or to a court or tribunal;
- e) it is reasonable to disclose the information to lessen or prevent a serious threat to the life, health, or safety of any individual, or to public health or safety;
- f) where, if ECC were bound by the Australian Privacy Principles or was an "APP entity", such use or disclosure would be permitted;
- g) the purpose for which it is to be used or disclosed is to provide Students, prospective Students, alumni, Staff, volunteers, and the community with information which may be useful and relevant to them, or about products, services and events provided by or on behalf of ECC, its partners, and affiliates;
- h) the College Director and Principal has authorised the use or disclosure having regard to the College's legal obligations, the functions of ECC as an Institute of Higher Education and the likely effect of such disclosure; or
- i) all of the following apply:

- i. the use is related to research or analysis that is in the public interest; and
 - ii. it is not practicable to obtain the agreement of each person that is the subject of the Personal Information before the use or disclosure.
- 4.10 Without limiting the above, and subject to paragraphs 4.12 and 4.13 relating to Sensitive Information, ECC may:
 - a) disclose Personal Information to various government agencies, including for purposes concerning Student eligibility for support services and payments such as loans under the [Higher Education Support Act 2003 \(Cth\)](#), scholarships, and Centrelink payments;
 - b) disclose Personal Information to a third party which is:
 - i. a related body corporate;
 - ii. a placement host or Work Integrated Learning provider;
 - iii. collaborating with the University (e.g., collaborative research or jointly delivered Courses);
 - iv. engaged by the University to assist with the University's functions or activities, including the provision or enhancement of services, refinement and accuracy of its information or data, determining Student matters (e.g. study applications, conduct), or similar; or
 - v. a student exchange or study abroad partner, transnational education services agreement partner, pathway provider, sponsor, education agent, or similar,ensuring that wherever practicable, appropriate contractual or technological safeguards will be established to protect Personal Information disclosed;
 - c) use and disclose Personal Information collected about a prospective Student for the purposes of assessing the effectiveness of marketing or to assist with future marketing;
 - d) use and disclose Personal Information collected about a prospective or current Staff member for the purposes of assessing employability and suitability, including to undertake or verify relevant background checks, or for compliance and accreditation purposes;
 - e) use and disclose Personal Information to maintain the ECC's graduate verification service;
 - f) disclose Personal Information where it is required by the College's external advisers (including external lawyers, insurers, risk advisers);
 - g) disclose Personal Information to a person's next of kin, guardian, or legal representative; or
 - h) if ECC is a contracted service provider for a Commonwealth contract, use or disclose Personal Information as necessary to meet an obligation under the contract.

Use and Disclosure of Sensitive Information (including Health Information)

- 4.11 ECC recognises that Sensitive Information, which includes Health Information, generally requires a higher level of privacy protection. Without limiting the above, the College will ensure that Sensitive Information is appropriately safeguarded, particularly for storage, record keeping, access, and determining whether disclosure is reasonable. Where disclosure occurs, ECC will take such steps as are reasonable in the circumstances to ensure the information is de-identified.
- 4.12 ECC may use or disclose Sensitive Information where:
- a) the person whom the information is about has expressly or by inference consented to its use or disclosure;
 - b) it is required or authorised by Australian law, a health direction, or a court or tribunal order;
 - c) it is reasonable to expect ECC to use or disclose the Sensitive Information for a purpose which is directly related to the primary purpose for which the information was collected;
 - d) it is reasonable in the circumstances to disclose the information to entities or bodies such as government agencies, statutory boards, law enforcement agencies, accreditation or registration bodies, independent oversight bodies, regulators, mediators, or conciliators, or to a court or tribunal;
 - e) it is reasonable to disclose the information to lessen or prevent a serious threat to the life, health, or safety of any individual, or to public health or safety;
 - f) it is reasonable to disclose the information to a person's next of kin, guardian, or legal representative; or
 - g) if the College were bound by the Australian Privacy Principles or was an "APP entity", such use or disclosure would be permitted.

Overseas Privacy Obligations

- 4.13 ECC may need to disclose Personal Information overseas, in accordance with the terms of this Policy, without contacting individuals to whom the Personal Information may relate, where the College has taken appropriate steps to adequately safeguard the Personal Information having regard to the particular circumstances. This includes the provision of Personal Information or Sensitive Information to third parties who may be located overseas and who are providing services to ECC, such as website hosts or software providers.

Direct Marketing

- 4.14 ECC may use or disclose Personal Information, other than Sensitive Information, for the purpose of direct marketing if:
- a) all of the following paragraphs (i)-(iv) apply:
 - i. the College collected the Personal Information from the individual;
 - ii. the individual would reasonably expect the University to use or disclose the Personal Information for the purpose of direct marketing;

- iii. the College provides a simple means by which the individual may easily request not to receive direct marketing communications; and
 - iv. the individual has not made such a request; or
- b) all of the following paragraphs (i)-(v) apply:
- i. the College collected the Personal Information from the individual and the individual would not reasonably expect the College to use or disclose the Personal Information for the purpose of direct marketing, or the College collected the Personal Information from someone other than the individual;
 - ii. the individual has consented to the use or disclosure for the purpose of direct marketing, or it is impracticable to obtain that consent;
 - iii. ECC provides a simple means by which the individual may easily request not to receive direct marketing communications;
 - iv. the College includes a prominent statement that the individual may make such a request, or draws the individual's attention to the fact that the individual may make such a request; and
 - v. the individual has not made such a request.

Data Breach Management

- 4.15 Staff must complete a Service Desk notification and notify their Line Manager if they become aware that:
- a) Personal, Sensitive or Health Information may have been lost, accessed by, or disclosed to, an unauthorised third party, or there is a real risk that Personal Information will be lost, accessed by, or disclosed to, an unauthorised third party; or
 - b) there has been a Cyber Security Incident involving ECC, or there is a real risk of a Cyber Security Incident involving ECC occurring.
- 4.16 Students should contact their Unit Coordinator if they become aware that:
- a) Personal, Sensitive or Health Information in their management or control as part of their College activities (in particular research activities), may have been lost, accessed by, or disclosed to, an unauthorised third party, or that there is a real risk that such Personal Information will be lost, accessed by, or disclosed to, an unauthorised third party; or
 - b) there has been a Cyber Security Incident involving ECC, or there is a real risk of a Cyber Security Incident involving ECC occurring.
- 4.17 In the event that ECC believes or suspects that personal data has been accidentally or unlawfully accessed, lost, disclosed, altered or destroyed, ECC will:
- a) inform Navitas and follow Navitas' *Data Breach Reporting and Management Procedure* if the issue is connected to Navitas IT services;
 - b) inform Edith Cowan University and follow ECU's [Data Breach Response Procedure](#) if the issue is connected to ECU IT services;

- c) where the data breach concerns both parties and/or where the extent of the problem is not yet known, ECC will inform both ECU and Navitas and will follow both of its partner policies during the resolution process.

Access to and Correction of Personal or Health Information

- 4.19 ECC will take such steps (if any) as are reasonable to ensure that Personal Information it collects, uses, or disclosures, is accurate, up-to-date and complete.
- 4.20 Requests for access and correction to Personal Information should be directed to Student and Academic Services.
- 4.21 ECC will generally provide individuals with access to their own Personal Information; however, there may be instances where ECC may limit or refuse access to this information, for example where the information includes third party Personal Information.
- 4.22 Where individuals ask for their Personal Information to be corrected, ECC will make the requested correction where it is reasonable to do so. If ECC determines that it would not be reasonable to correct an individual's Personal Information, individuals may apply under the [Freedom of Information Act 1992 \(WA\)](#) for an amendment of Personal Information.
- 4.23 ECC will refer to its legislative and ethical requirements, the exceptions set out in the Australian Privacy Principle 12 and 13, the need for reasonableness, College Policies and Procedures (including human resources processes), and its contractual obligations, to assess whether access to information is appropriate, and whether it is reasonable for the College to notify third parties of corrections to be made.
- 4.24 Access and use of Personal Information within ECC will only be by Staff who would reasonably be expected to be privy to such information, and who have a need to use it to carry out the College's functions or activities.

Privacy Complaints

- 4.25 Complaints from Students regarding the ECC's handling of Personal, Sensitive and Health Information will be addressed in accordance with the [Student Complaints Policy](#).
- 4.26 Complaints from Staff regarding the ECC's handling of Personal, Sensitive and Health Information will be addressed in accordance with Navitas' [Grievance Management Policy](#).
- 4.27 Complaints regarding the ECC's handling of Personal, Sensitive and Health Information from persons external to ECC will be referred to the College Director and Principal.

5. ACCOUNTABILITIES AND RESPONSIBILITIES

5.1 All ECC Staff and Students are responsible for complying with this Policy.

6. RELATED DOCUMENTS:

6.1 ECC Policies related to this Policy include:

[Staff Code of Conduct](#)
[Student Complaints Policy](#)
[Student Conduct Policy](#)

6.2 Navitas Policies related to this Policy include:

[Data Protection Policy](#)
[Records Management, Retention and Disposal Policy](#)
[Information Security Policy](#)

6.3 ECU Policies related to this Policy include:

[Cyber Security Incident Response](#)
[Data Breach Response Procedure](#)
[Privacy Policy](#)

6.4 This Policy has been developed in line with requirements set out in the:

[Freedom of Information Act 1992](#)
[Higher Education Support Act 2003](#)
[Privacy Act 1988](#)
[Australian Privacy Principles](#)

7. CONTACT INFORMATION:

For queries relating to this document please contact:

POLICY OWNER	College Director and Principal
ALL ENQUIRIES CONTACT:	Quality and Compliance Manager
TELEPHONE:	08 6279 1133
EMAIL ADDRESS:	justask@ecc.edu.au

8. APPROVAL HISTORY:

POLICY APPROVED BY:	Senior Management Group
DATE POLICY FIRST APPROVED:	November 2007
DATE LAST MODIFIED:	June 2018
REVISION HISTORY:	February 2023. Adoption of a principle-based approach to policy and closer alignment with ECU's <i>Privacy Policy</i> . Inclusion of new information on Data Breach Management. November 2023. Removal of Partner Provider due to localization of policy in Sri Lanka.
NEXT REVISION DUE:	November 2025