Employee Records Privacy Policy

Section 1 - Policy Purpose

(1) The purpose of the privacy policy is to protect private information about individuals and to ensure that the University conforms with the Privacy Amendment (Private Sector) Act 2000 (Cth), and the National Privacy Principles of the Act.

Section 2 - Employee Record Defined

(2) An employee record is a record of personal information either conventional or in electronic format relating to the employment of a staff member. The record comprises information about employment, including health, recruitment and selection, terms and conditions of employment, performance, discipline, and resignation. Employees records are confidential and kept in locked storage. Employee records are exempt records from the provisions of the Privacy Amendment (Private Sector) Act 2000 (Cth). The formal employee record exists within People and Capability.

Section 3 - Policy Provisions

Collection of Information

(3) Personal information must only be collected for purposes necessary to the functions and activities of the University. These include:

a. selection,
b. employment,
c. appraisal,
d. discipline,
e. remuneration of staff, and
f. University administrative activities.

(4) Personal information must only be collected by means that are permissible by law.

(5) When personal information is collected by the University, the University must clearly state:

a. the fact that the information is being collected;
b. the purposes for which the information is being collected;
c. the intended recipients of the information;
d. whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information is not provided; and,
e. the existence of any right of access to, and correction of, the information.

(6) When the University collects personal information from a staff member, the University must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

a. the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete; and
b. the collection of the information does not intrude to an unreasonable extent on the personal affairs of the staff member to whom the information relates.

(7) Where reasonably possible, the University will only collect personal information directly from the staff member to whom the information relates. Frequently this will be collected from official University forms but it may also be collected from email, letters or other forms of communication. However, the staff member may authorise the collection of information from a third party or, in the case of a person under the age of 16, authorisation may be given by a parent or guardian of that person.

(8) If the University collects personal information about a staff member from a third party, reasonable steps must be taken to ensure that the staff member is or has been made aware of the collection and the reason for the collection.

(9) The University will employ best practice in soliciting or collecting information from individuals using electronic forms or e-mail. The risks associated with using the Internet as a transmission medium will be made clear and the individual will be notified of any other options available for providing the information required.

Use of Information

(10) The University must not use the information for a purpose other than that for which it was collected unless:

a. the staff member to whom the information relates has consented to the use of the information for that other purpose;
b. the other purpose for which the information is used is directly related to the purpose for which the information was collected;
c. the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person; or,
d. if so directed by a court of law.

(11) If the University uses or discloses personal information (authorised above), it must make a written note of the use of disclosure and of the reason for its disclosure.

Access to Information

(12) Current and previous staff members are entitled to know whether personal information about them is held by the University, the nature of the information, the main purposes for which it is used and their entitlements to gain access to it.

(13) Access to personal information includes opportunity for the staff member to inspect records, take notes or obtain a photocopy or computer print out however, this must be in the presence of a representative from People and Capability.

Access for the Individual

(14) The University will provide the staff member access to their personal employee record upon written request by the staff member, except:

a. in the case of personal information, other than health information, providing access would pose a serious and imminent threat to the life or health of any staff member;
b. providing access would have an unreasonable impact upon the privacy of other staff members;
c. the request for access is frivolous or vexatious;

d. providing access would reveal the intentions of the organisation in relation to negotiations with the staff member in such a way as to prejudice those negotiations;
e. providing access would be likely to prejudice an investigation of possible unlawful activity;
f. denying access is required or authorised by or under law; and,
g. providing access would be likely to prejudice the outcome of an internal investigation.

(15) Access to employee records is provided to the staff member, nominated supervisor or Executive Team member for positions in their line of responsibility.

(16) If the University is not required to provide the staff member with access to the information because of one or more of (the above) reasons, the University must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

Access for Others

(17) The University will not disclose personal information to anyone or any organisation, unless:

a. the disclosure is related to the purpose for which the information was collected. There must be no reason to believe that the staff member concerned would object to the release of the information;
b. the staff member concerned was reasonably likely to have been aware, or had been notified, that the personal information is usually disclosed to the person or agency;
c. the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of any person;
d. in relation to some investigations and law enforcement process; and
e. where legislation recognises lawful access by some government agencies.

(18) The University must provide reasons for denial of access or a refusal to correct personal information.

Provision of Information

(19) The University will respond to a staff member's written and signed request for their personal information as soon as practicable.

(20) The time taken to respond to a staff member's request for access may be influenced by various factors. These may include the method of communication, the type or amount of personal information requested, how the personal information is held, if a third party needs to be consulted and how it is to be provided to the individual making the request.

Access and Law Enforcement

Police

(21) Requests for information from the police will not be accepted over the telephone. Members of staff receiving written requests for personal information from law enforcement agencies must direct the inquirer to the Chief Operating Officer or delegate.

(22) This procedure does not apply in cases where there is an imminent threat to life or safety. However, even then reasonable attempts should be made to discuss the matter with the Chief Operating Officer or delegate. In most other circumstances it may be assumed that the University will require the issuing of a search warrant or subpoena. Records of all requests and disclosures of personal information to the law enforcement agencies will be kept on the appropriate file maintained by People and Capability.

Government

(23) Departments such as Social Security, Immigration and Ethnic Affairs, Taxation and ASIO sometimes have a lawful need to access personal information held by the University. Where this need exists it is recognised in the legislation which establishes the departments and regulates their functions. While the University wishes to be cooperative with the Commonwealth, it has a duty to its staff. Therefore, any Commonwealth Department requiring personal information should be informed that the University will supply personal information only in response to a formal notice under the Department's legislation.

Subpoenas and Court Orders

(24) The personal information held by the University is often required as evidence in court and tribunal proceedings. These may be matters which do not involve the University, or litigation to which the University is joined as a party. For all matters, the Proper Officer to be named in subpoenas and other orders is the Chief Operating Officer or delegate. Subpoenas received by the University must be directed to the office of the Chief Operating Officer and if necessary, will then be directed to General Counsel.

Security

(25) The University will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

(26) The University must approve the use of personal computers in the workplace or for the copying or transferring of personal information onto personal computers. At the time of separation from the University, the University will take all appropriate steps to identify personal information stored on personal computers and direct and supervise the removal of personal information.

Communication

(27) This Policy will be distributed to all existing staff and new staff of the University.

Breach of the Privacy Policy

(28) This Policy is designed to promote and enhance the confidentiality of ACU staff in the workplace. A failure to comply with this policy will be viewed seriously and may, in line with the enterprise agreement(s) in place at the time, result in disciplinary action, including dismissal.

(29) Staff must report breaches of this policy to the Chief Operating Officer or delegate, who is responsible for the application of legislation.

(30) The University will use its utmost endeavours to protect staff who, in good faith and with good grounds, report breaches of the Privacy Policy.

Grievances

(31) Any grievance arising from the application of these arrangements shall be managed using the grievance management process foreshadowed in the ACU Staff Enterprise Agreement 2022-2025. In the interim, any unresolved issue should be raised in the first instance with the relevant supervisor. If the nominated supervisor is unable to resolve the matter, it may be referred to the relevant Executive Team member.

Section 4 - Policy Review

(32) The University may make changes to this policy from time to time to improve the effectiveness of its operation. In this regard, any staff member who wishes to make any comments about this policy may forward their suggestions to the Chief People Officer.

Section 5 - Further Assistance

(33) Any staff member who requires assistance in understanding this Policy should consult their nominated supervisor who is responsible for the implementation and operation of these arrangements in their work area. Should further information or advice be required staff should visit Service Central.

Section 6 - Associated Information

(34) For related legislation, policies, procedures and guidelines and any supporting resources please refer to the Associated Information tab.

Status and Details

Status	Current
Effective Date	19th December 2023
Review Date	30th April 2024
Approval Authority	Vice-Chancellor and President
Approval Date	19th December 2023
Expiry Date	Not Applicable
Responsible Executive	Angelle Laurence Chief People Officer
Responsible Manager	Angelle Laurence Chief People Officer
Enquiries Contact	Bernardine Lynch ER and Safety Committees and Policy Officer People and Capability