Third Party Access to Personal Information Protocol

Section 1 - Purpose and Scope

(1) This Protocol should be read in conjunction with the Privacy Policy and supports the application of Section 5, clauses 18 to 21 of that Policy.

(2) This Protocol also supports the application of clause 3 of the Employee Records Privacy Policy regarding use and access.

(3) This Protocol outlines the internal processes relating to third party requests for personal information of staff or students.

(4) The term third party is used in this Protocol to refer to external bodies (organisations or persons) as well as ACU staff members who would not ordinarily be authorised to access the personal information of students or other staff members in the performance of duties associated with their employment.

(5) All other terms used in this Protocol have the same meaning as defined in Section 9 of the Privacy Policy.

(6) Under Australian Privacy Principle 12, an individual (or another authorised person acting on behalf of the individual) has the right to request access to their own personal information held by the University. This Protocol does not apply to these requests; they are managed in accordance with clause 28 of the Privacy Policy and the Access to and Correction of Personal Information Procedure.

Section 2 - Use or Disclosure of Personal Information

(7) Australian Privacy Principle 6 requires organisations holding personal information not to use or disclose it other than for the purpose for which it was collected.

(8) ACU staff must have a demonstrated need for access to student or staff personal information to undertake their functions or responsibilities.

(9) A data breach occurs where there has been unauthorised use or access to personal information (within ACU) or unauthorised disclosure of personal information (outside of ACU).

Section 3 - Release of Personal Information

(10) The personal information of staff or students must not be released to third parties (which may include ACU staff members or external bodies) unless:

a. notice given at the time of collection advises the individual about the specific use or disclosure (primary purpose); or
b. consent is obtained from the individual; or

c. one of the following exceptions apply under the Privacy Act 1988 (Cth) and the Privacy Officer authorises the use or disclosure:
    i. the individual would reasonably expect ACU to use or disclose their personal information for a secondary purpose directly related to the primary purpose;
    ii. The disclosure is required or authorised by law e.g court order, subpoena, statutory provision.
d. ACU reasonably believes the use or disclosure is necessary for the investigation, enforcement or prosecution of criminal matters or breaches of law;
e. ACU reasonably believes the use or disclosure is necessary to manage or lessen a serious threat to a person's life, health, safety, or welfare, or to public health, safety or welfare and it is unreasonable or impracticable to obtain consent;
f. ACU has reason to suspect that unlawful activity or serious misconduct has occurred in relation to its functions or activities and reasonably believes that the use or disclosure is necessary to internally investigate or take action;
g. ACU reasonably believes the use or disclosure is necessary to locate a person reported as missing;
h. ACU reasonably believes the use or disclosure is necessary for conducting an alternative dispute resolution process.

Section 4 - Assessment of Requests and 'Reasonable Belief' Requirement

(11) The scenarios described in clause 10(c). generally require ACU to have a reasonable basis for the belief that the use or disclosure is necessary in the circumstances.

(12) The third party must provide sufficient information to enable the Privacy Officer to form a view as to whether there are reasonable grounds to believe disclosing the information is necessary. This includes:

a. setting out the basis upon which authorisation for the release of information is sought; and
b. specifying what information is required and why it is needed.

(13) It is the responsibility of ACU to obtain and document evidence to justify this belief.

(14) The Office of the Australian Information Commissioner advises that this must not be a subjective belief and it would not be considered necessary where it is merely helpful, desirable or convenient. Case law [1] requires organisations to seriously consider whether any effective alternatives are available to disclosure, seeking further information from law enforcement bodies and ascertaining the legislative grounds authorising the disclosure.

> [1] Refer 'EZ' and 'EY' [2015]

(15) The Privacy Coordinator will assess the merits of each request, the grounds for 'reasonable belief' and the permissibility of disclosure. A recommendation will be provided to the Privacy Officer on a case by case basis. Factors to be considered include:

a. the nature of the personal information being requested (sensitive personal information is afforded a higher level of protection under the Australian Privacy Principles);
b. the authority of the requesting enforcement or government body;
c. the relevant exception referred to in clause 10(c) of this Protocol;
d. whether the incident occurred on ACU premises and the University is already aware of the circumstances

surrounding the request or investigation;

e. whether the incident concerns ACU property or involving ACU staff or students;
f. whether the matter was reported to the enforcement body by ACU staff or student; and
g. in relation to CCTV requests, whether the footage is likely to capture images of students or staff (location of the surveillance device, day and time of the alleged incident).

(16) The Privacy Coordinator may recommend further enquiries are made with the requestor and / or more information is sought in order to assess the third party request.

(17) The Privacy Officer may refuse to disclose information in the absence of a warrant, subpoena or similar legal order.

(18) Where ACU is not satisfied that the grounds for accessing or disclosing the information are met, then no legal basis under the Privacy Act 1988 (Cth) is met and the request will be denied.

(19) Where ACU is satisfied it has a reasonable basis for the belief, it must only disclose the minimum amount of personal information that is necessary.

(20) A written record of the authorised use of disclosure must be registered by the Privacy Coordinator.

Section 5 - Types of Requests

Student Records

(21) The Student Enrolment Privacy Collection Statement sets out the various ways in which ACU may use and disclose students' personal information.

(22) Where a third party requests access to a student record and the use or disclosure is not already provided for in the Collection Statement, a determination will need to be made as to whether any of the circumstances in clause 10 of this Protocol apply. Refer to clauses 31-33 for requests specifically from law enforcement agencies.

(23) A staff member who receives a request under clauses 21-25 should seek direction from the Academic Registrar in the first instance.

(24) The Academic Registrar may refer it to the Privacy Coordinator for advice or to seek authorisation from the Privacy Officer to use or disclose the information under clause 10(c).

(25) The Privacy Coordinator will assess the request in accordance with clauses 11 to 20 of this Protocol and brief the Privacy Officer.

Staff Employment Records or Recruitment Records

(26) The Employee Records Privacy Policy and Privacy Collection Notice Requirements for Applicants and Referees set out the various ways in which ACU may use and disclose personal information for staff (or prospective staff).

(27) Where a third party requests access to a staff record and the use or disclosure is not already provided for in the Collection Notice a determination is needed as to whether any of the circumstances in clause 10 of this Protocol apply. Refer to clauses 31 to 33 for requests specifically from law enforcement agencies.

(28) A staff member who receives a request under clauses 26 to 30 should seek direction from the Chief People Officer in the first instance.

(29) The Chief People Officer may refer it to the Privacy Coordinator for advice or to seek authorisation from the

Privacy Officer to use or disclose the information under clause 10(c).

(30) The Privacy Coordinator will assess the request in accordance with clauses 11 to 20 of this Protocol and brief the Privacy Officer.

Law Enforcement Agencies

(31) ACU may receive requests from law enforcement agencies for the disclosure of personal information. Where the request relates to CCTV refer to clauses 35 to 38.

(32) A list of relevant law enforcement bodies and law enforcement activities are set out in Section 6 of the Privacy Act 1988 (Cth).

(33) A staff member who receives a request under clauses 31 to 33 should refer it to the Privacy Coordinator who will assess the request in accordance with clauses 11 to 20 of this Protocol and brief the Privacy Officer.

Emergencies and Critical Incidents

(34) In cases of emergency or where a Critical Incident is declared under the Critical Incident Management Policy, the Critical Incident Convenor may:

a. seek the advice from the Privacy Coordinator; or
b. authorise the use or disclosure and subsequently notify the Privacy Coordinator for the purposes of making a record as per clause 20.
c. In circumstances where an Incident is declared under the Critical Incident Management Policy and access or disclosure of personal information appears necessary to manage the incident, the Incident Convenor should contact the Privacy Coordinator to:
    i. seek advice; or
    ii. request authorisation from the Privacy Officer to use or disclose the personal information under clause 10(c);
    iii. if authorisation is granted by the Privacy Officer under 34(c)(ii) then the Incident Convenor is authorised to establish the necessity for other staff members to access the personal information (e.g for investigative purposes).

Closed Circuit Television Vision (CCTV) Footage and Door Reader Access Reports

(35) Where an internal or external request for CCTV footage or door access report is received by Properties and Facilities, the Associate Director, Facilities Management may direct the National Security Centre to retrieve and copy (but not release) the footage or report [2].

> [2] Be aware that footage is not retained for more than 30 days so will be unavailable if this period has elapsed.

(36) The Associate Director, Facilities Management will forward the request to the Privacy Coordinator who will assess the request in accordance with clauses 11-20 of this Protocol [3] and brief the Privacy Officer.

> [3] This may also require an assessment against workplace surveillance legislation, where applicable.

(37) Only when the Associate Director, Facilities Management receives confirmation of this authorisation via the

Privacy Coordinator, shall Properties and Facilities coordinate with the National Security Centre to obtain the footage and release it.

(38) For the avoidance of doubt, and with reference to clause 4 of this Protocol, requests by Campus Facilities Managers for CCTV footage or door access reports would be considered requests within the normal performance of their duties and can be managed by the Director or Associate Director of Properties and Facilities. This access would be limited to the staff member and no disclosure is permitted. If the request includes disclosure to a third party (which may include unauthorised ACU staff members or external bodies) then clauses 36 and 37 of this Protocol apply.

Ask ACU and Service Central Telephone Recordings

(39) A pre-recorded privacy statement is available for AskACU and Service Central and sets out the purpose of the recordings and how they may be used. This relates to quality, coaching and training purposes.

(40) Where a third party is requesting access to a recording and the use or disclosure does not relate to one of these purposes then a determination will need to be made as to whether any of the circumstances in clause 10 of this Protocol apply.

(41) A staff member who receives a request under clauses 21 to 25 should seek direction from the Academic Registrar (if the recording involves student personal information) or the Chief People Officer (if the recording involves staff personal information) in the first instance.

(42) The Academic Registrar or Chief People Officer may refer it to the Privacy Coordinator for advice or to seek authorisation from the Privacy Officer to use or disclose the information under clause 10(c).

(43) The Privacy Coordinator will assess the request in accordance with clauses 11 to 20 of this Protocol and brief the Privacy Officer.

(44) Unless otherwise indicated, this Protocol will still apply beyond the review date.

Status and Details

Status	Current
Effective Date	2nd April 2024
Review Date	30th April 2024
Approval Authority	Director, Governance
Approval Date	2nd April 2024
Expiry Date	Not Applicable
Responsible Executive	Diane Barker Director, Legal, Assurance and Governance
Responsible Manager	Matthew Charet National Manager, Governance
Enquiries Contact	Natalie Koppe Privacy Coordinator Legal, Assurance and Governance Directorate