Personal Information Access Procedures

Table of Contents

1. Governing Policy

Privacy Policy

2. Purpose

To describe the process when individuals seek access to their own personal information held by the University.

3. Definitions

personal information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not, or as otherwise defined by applicable data protection laws
sensitive information	any personal information that is about a person's a. health, health treatment, or other medical needs b. race, ethnicity or religion c. professional or political affiliations and memberships d. criminal record e. sexuality f. disability status g. religious or philosophical beliefs h. trade union membership, or i. genetic or biometric data.
personnel	For the purposes of these procedures, **personnel** includes staff, students, academic status holders, volunteers, contractors, University agents and associated third parties,

4. Procedures

4.1. Individuals seeking access to their own personal information

a. In most cases and subject to verification of identity, all individuals have a right to access, correct, or update their personal information held by the University.

b. University personnel must respond to requests for access or correction in a timely manner (and in any event within 30 days).

c. Individuals can seek access or request a correction or update as follows:

   i. Current and former students can access their personal information in accordance with the relevant provisions of the Student Information Management Procedures.

   ii. Employees and academic status holders can contact People and Culture to make an appointment to view their staff file in the presence of a People and Culture officer. Requests to view or access other employment-related information should be directed to the relevant data controller (such as the administrator of the IT system in which the data is held).

   iii. Persons other than staff, affiliates or current or former students seeking access to personal information held by the University about them should contact the relevant business area to whom the information was provided in accordance with section 11 of the University's Privacy Policy.

d. Identity verification requirements include:

   i. In person—picture ID e.g., student or staff card or driver's licence

   ii. By telephone—questions to verify a range of details, e.g., FAN, Student or staff ID, Date of Birth, Course, address

   iii. Via email, other than a Flinders University e-mail address—the person will be asked to log in using their FAN and password to authenticate themselves and submit their request via their Flinders email. If the person no longer has a Flinders email address, verification will be by asking a series of questions, as above.

4.2. Limitations on Access

a. Documents may be withheld or redacted if the University determines that it would not be appropriate for access to be granted. Access by an individual to their personal information may be denied for the following reasons:

   i. there would be an unreasonable impact on the privacy of other individuals (e.g. personally identifying information of referees on a staff appointment file)

   ii. the request for access is frivolous or vexatious

   iii. the documents are subject to confidentiality obligations or legal professional privilege

   iv. granting access would compromise the University in anticipated legal proceedings or commercially sensitive decision-making processes, or

   v. there is a potential threat to life, health or safety.

b. An individual who is denied access to a document or who has had their correction request refused must be given reasons for the refusal and should be advised of their entitlement to submit a Freedom of Information application.

Example: *A student seeks copies of correspondence between the University and its solicitors concerning a legal matter involving the student. Correspondence between the University and its solicitors is subject to legal professional privilege and should not be released.*

A student seeks copies of correspondence between two lecturers concerning accusations about the student's behaviour. The student should seek the information under the Freedom of Information Act.

A lawyer claiming to act for a student seeks that student's academic record. The student must provide written consent for that information to be released.

If a lawyer is acting in a court case against a student or a staff member, personal information may only be released to the lawyer if the court issues a subpoena or similar order.

4.3. Third parties seeking access to personal information

a. Permitted disclosures to third parties are set out in section 7 of the Privacy Policy. The examples listed below address some common requests for access from third parties.

b. Access to Student Personal information must be in accordance with relevant provisions of the Student Information Management Procedures.

c. Any request from the police for access to any person's personal information, or the presentation of any form of warrant by police, must be referred to Legal Services for advice. Legal Services will provide advice to the relevant senior manager on the release of any information or action to be taken.

d. Requests for access by **Government agencies** should cite the authority upon which the request is made. If uncertain about the bona fides of the request, seek advice from Legal Services before releasing any information.

e. personal information must not be disclosed in response to a **lawyer's** request except with the consent of the person to whom the information relates, or if required by law or a subpoena or court/tribunal order.

Examples: *A member of the public contacts a staff member and asks for the contact details of another staff member. The contacted staff member may refer the caller to the Staff Directory, as it is publicly available information. If the caller wants private information, the caller's contact details will be taken, and referred on to the relevant staff member who can then choose whether to contact the caller.*

A member of the public claiming to be the relative of a student contacts a staff member to seek information about the student. The staff member will not provide any information, or even acknowledge that the person inquired about is a student, except where the student has given written permission for specified information to be released to specified individuals. Where permission has been given, the staff member must verify the caller's identity first and then make a record of the disclosure.

Police wish to know if a person is enrolled at the University and their study details. The police submit a warrant or police letter quoting the Act that entitles them to request the information or a letter from someone of suitable authority stating that the information is reasonably necessary for the investigation of an offence. Such matters will be referred to Legal Services for advice.

If a staff member is suspected of illegal activities, the University may disclose the staff member's personal information to the Police or other authorised investigator.

5. Right to erasure (right to be forgotten)

a. This Procedure applies only to personal information collected in respect of individuals located in the European Union (EU), due to the application of Regulation EU (2016/679)–General Data Protection Regulation (GDPR).

b. Under the GDPR, there is a right for individuals to have their personal information that has been collected by the University erased from the University's records. This right is often referred to as the *"right to be forgotten" or "right of erasure"*. The right is not absolute and only applies in certain circumstances.

c. The steps required for the University to give effect to an individual's right to erasure will vary depending on:
   i. where the personal information that is the subject of the request is held, and/or
   ii. to whom it has been disclosed.

d. The timeframe for responding to the individual in respect of the request for deletion must not exceed **one month** from the date on which the request was first received by the University.

e. Any request for personal information to be deleted must be submitted within 48 hours to the Privacy Officer via email at privacy@flinders.edu.au.

f. The Privacy Officer will be responsible for reviewing and assessing the request, including by:

i. identifying whether the request relates to EU Personal Data
ii. liaising with the relevant business unit to determine what personal information is held by the University and in what databases or locations the information is located
iii. consulting with the relevant stakeholders in respect of the personal information held and the purposes for which it is held
iv. making an assessment of whether the University is required to delete the personal information under the GDPR, including whether any exemption applies
v. providing advice to the relevant senior manager as to whether or not deletion of the individual's personal information (in whole or in part) is required, and
vi. approving the response to the individual who made the request for their personal information to be deleted.

g. Once erasure is approved by the Privacy Officer, Information & Digital Services will be responsible for undertaking searches and/or erasure of electronic information.

h. The relevant senior manager/s of the business unit/s holding personal information about the applicant must provide prompt assistance to the Privacy Officer and IDS in respect of any request for deletion of personal information.

i. Any recommendation to delete personal information in accordance with this procedure, and any communication to the relevant individual making the request, must be approved in writing by the Privacy Officer.

Approval Authority	University Secretary
Responsible Officer	General Counsel, Governance, Legal & Risk
Approval Date	3 December 2018
Effective Date	3 December 2018
Review Date*	December 2021
HPRM file number	CF18/1065
* Unless otherwise indicated, this procedure will still apply beyond the review date.	