Email and Electronic Data Access Procedures

Table of Contents

1. Governing Policy

Information Security Policy

2. Purpose

To define the process for authorising access to, or retrieval of, user data, including email and/or personal storage data, to meet specific legal or operational requirements.

3. Provision of access

a. Requests by former staff and students to their own data are generally approved unless the circumstances of their departure create legal, ethical or administrative issues that prevent the granting of access.

b. Requests by third parties to access the accounts or data of any current or former University IT System User are generally denied, unless compelling justification can be supplied, including any of the following:

   i. Express written permission from the user in question

   ii. Express written approval from Deputy Vice Chancellor (Students), Director People and Culture (staff) or Chief Information Officer (other)

   iii. Request from a law enforcement agency as part of an investigation

   iv. Court order

   v. Freedom of Information request (Freedom of Information Act (South Australia) 1991).

b. All approved access requests are granted on a temporary basis.

4. Procedures

4.1. Request to access own data

Former Staff Member or Student	a. Submit the data access request to ictsecurity@flinders.edu.au. b. Provide an estimate of the amount of time access is required. c. Provide justification for the access request.
Information Security and Governance Representative	d. Validate requester's identity (e.g. Name, date-of-birth and address). e. Assess whether denying the request would have an adverse impact on the requester. f. Identify whether fulfilling the request creates potential for conflict-of-interest issues or legal issues for the University. g. Assess whether requester was dismissed from the University for breaches of policy. h. Assess level of effort required to recover the requested data. i. Record data access request in the University's service management tool. j. If all questions answered favourably, forward request and associated assessment to Director, People and Culture (Staff) or Deputy Vice Chancellor (Students) for approval.
Director, People and Culture OR DVC (Student)	k. Assess the merits of the application based on the analysis provided. l. Approve or deny the request and communicate decision back to Information Security staff member.
Information Security Staff Member	m. Communicate decision to access requester. n. If access approved, forward request to Information & Digital Services support staff for fulfilment.

4.2. Request to access another user's data

Requester	a. Submit the data access request to ictsecurity@flinders.edu.au. b. Provide the name of the person who is the subject of the request. c. Provide an estimate of the amount of time access is required. d. Provide details of the data or email to be accessed (e.g. dates, headers, subject, key words) to allow for easier identification. e. Provide justification for the access request (e.g. written permission from data owner or from relevant College/Portfolio Head; court order, freedom of information request).

Information Security and Governance Representative	a. Identify the subject of the access request by matching known attributes (e.g. name, date-of-birth, address, student number, HR number). b. Assess whether denying the request would have an adverse impact on the requester or on the University. c. Identify whether fulfilling the request creates potential for conflict-of-interest issues or legal issues for the University. d. Assess level of effort required to recover the requested data. e. Record data access request in the University's service management tool. f. If all questions answered favourably, forward request and associated assessment to Director People and Culture (Staff), Deputy Vice Chancellor (Students) or CIO (other) for approval.
Director, People and Culture OR DVC (Student) OR Chief Information Officer (Other)	a. Assess the merits of the application based on the analysis provided. b. Engage Governance and Legal Unit (legal@flinders.edu.au) to ensure no legal issues would prevent the granting of access. c. Approve or deny the request and communicate decision back to Information Security staff member.
Information Security Staff Member	d. Communicate decision to access requester. e. If access approved, forward request to Information & Digital Services support staff for fulfilment.

5. Supporting documentation

Freedom of Information

Approval Authority	Vice-President (Corporate Services)
Responsible Officer	Chief Information Officer
Approval Date	21 December 2017
Effective Date	21 December 2017
Review Date*	December 2020
HPRM file number	CF16/50

* Unless otherwise indicated, this procedure will still apply beyond the review date.