Email and Electronic Data Access Procedures

Table of Contents
1. Governing Policy
2. Purpose
3. Definitions
4. Procedures
   4.1. Provision of access
   4.2. Requesting access
5. Supporting documentation

1. Governing Policy

Digital Security Policy

2. Purpose

To outline the process for authorising access to, or retrieval of, the data of current and former Flinders University community members, including email and/or data storage, to meet specific legal or operational requirements.

3. Definitions

<table>
<thead>
<tr>
<th>Email</th>
<th>Message(s) distributed by electronic means from one computer user to one or more recipients via a network as provisioned by the University. These messages can contain text, text and files or files only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data storage</td>
<td>Devices used to save and/or enable access to collections of data in an electronic format.</td>
</tr>
</tbody>
</table>

4. Procedures

4.1. Provision of access

Access to University-provided email and/or data storage will cease on the end date of a FAN account holder's employment or enrolment.

4.1.1. Former staff and contractors

a. After their employment has ceased, former staff and contractors with no ongoing status with the University will not be granted access to University-provided email and/or data storage.

b. A current staff member may be authorised to access University-provided email and/or data storage of a former staff member or contractor, in the form of an export of the requested information, if there are compelling circumstances.

c. The compelling circumstances in which access may be authorised include:

   i. a request from a law enforcement agency as part of an investigation
   ii. a court order
   iv. other compelling circumstances, as approved by the relevant authority.
4.1.2. Former students

a. After their enrolment has ceased, former students may be authorised to access University-provided email and/or data storage, in the form of an export of the requested information, if there are compelling circumstances.

b. The compelling circumstances in which access may be authorised include:
   i. a request from a law enforcement agency as part of an investigation
   ii. a court order
   iv. other compelling circumstances, as approved by the relevant authority.

4.1.3. Third parties

a. Third parties may be authorised to access the University-provided email and/or data storage of a current or former FAN account holder if there are compelling circumstances, including:
   i. in the case of a current FAN account holder, express written permission from the account holder
   ii. in the case of a former FAN account holder, express written approval from the Director, People and Culture, Deputy Vice Chancellor (Students) or Chief Information Officer
   iii. request from a law enforcement agency as part of an investigation
   iv. a court order
   v. a Freedom of Information request (Freedom of Information Act (SA) 1991)
   vi. other compelling circumstances, as approved by the relevant authority.

4.2. Requesting access

<table>
<thead>
<tr>
<th>Requestor</th>
<th>a. Make a request to the assessor:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Includes current staff member, former student or third party)</td>
<td>i. supervisor of the former staff member, in the case of a current staff requestor</td>
</tr>
<tr>
<td></td>
<td>ii. Flinders Connect or the IDS Service Desk, in the case of a former student requestor</td>
</tr>
<tr>
<td></td>
<td>iii. IDS Service Desk, in the case of a third-party requestor.</td>
</tr>
<tr>
<td></td>
<td>b. Details of the request must include:</td>
</tr>
<tr>
<td></td>
<td>i. name of the subject of the request</td>
</tr>
<tr>
<td></td>
<td>ii. estimate of the amount of time that access is required (if relevant)</td>
</tr>
<tr>
<td></td>
<td>iii. details of the data or email to be accessed (e.g., dates, headers, subject, key words)</td>
</tr>
<tr>
<td></td>
<td>iv. the compelling circumstance for the access in accordance with s.4.1.1.c, s.4.1.2.b or s.4.1.3.a.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assessor</th>
<th>c. Identify the subject of the access (e.g., name, date-of-birth, address, student number, staff number, FAN).</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Supervisor, Flinders Connect or IDS Service Desk)</td>
<td>d. Assess the request, including whether:</td>
</tr>
<tr>
<td></td>
<td>i. denying the request would have an adverse impact on the requestor</td>
</tr>
</tbody>
</table>
ii. fulfilling the request creates a potential conflict of interest or legal issue for the University
iii. the requestor was dismissed from the University.
e. If supported, submit a data access request to Information Security via ServiceOne with an explanation of the compelling circumstance.

Information Security

f. Confirm the identity of the access request by matching known attributes (e.g., name, date-of-birth, address, student number, staff number, FAN).
g. Assess the level of effort required to recover the requested data.
h. If the request is validated, forward the request and associated assessment to the Approver:
   i. Director, People and culture in the case of former staff
   ii. Deputy Vice-Chancellor (Students) in the case of former students
   iii. Chief Information Officer in all other cases

Approver

i. Assess the merits of the request based on the analysis provided.
j. Approve or deny the request and communicate the decision back to Information Security staff member.

Information Security

k. Communicate the decision to the requestor.
l. If access approved, complete the request and provide access to requested data.

5. Supporting documentation

Freedom of Information

<table>
<thead>
<tr>
<th>Approval Authority</th>
<th>Vice-President (Corporate Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Officer</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Approval Date</td>
<td>31 July 2024</td>
</tr>
<tr>
<td>Effective Date</td>
<td>31 July 2024</td>
</tr>
<tr>
<td>Review Date*</td>
<td>2027</td>
</tr>
<tr>
<td>Last amended</td>
<td></td>
</tr>
<tr>
<td>CM file number</td>
<td>CF16/50</td>
</tr>
</tbody>
</table>

* Unless otherwise indicated, this policy or procedures still apply beyond the review date.