Access to user data policy

Responsibility of: Associate Pro-Vice Chancellor & Chief Information Officer
Approval Date: June 2018
Review Date: June 2020
Approved By: Vice Chancellor’s Executives
Section 1: Introduction

1.1 Data in UWL is stored both at the team/collaborative level and at the individual level.

- Examples of data stored at the team level would be data stored in shared network drives, in SharePoint, or in specific applications such as the Student Records system.
- Examples of data stored at the individual level would be data stored in OneDrive or the contents of an individual's email account.

1.2 As a general practice, data should not be stored at the individual level if other staff members will need to access it. It is the responsibility of staff members and teams to ensure data is stored in the appropriate place. For example, a team SharePoint site is ideal for storing documents that are to be worked on collaboratively by team members.

1.3 Where it is anticipated that another staff member will need access to data stored at the individual level, this should be arranged in advance. In particular, when a member of staff is leaving or changing their role in the university, they should work with their line manager in advance to ensure relevant data is moved to the appropriate place.

1.4 However, there will inevitably be situations where access to individual data is required by another member of staff, for example when an employee is unexpectedly absent due to illness.

Section 2: Policy

2.1 Access to an employee's data should normally be granted to others only with the employee's written consent.

2.2 If consent cannot be obtained, for example where a member of staff is on long term illness, then access will be granted only with the authorisation of the University Secretary and Chief Compliance Officer or, in her absence, a nominated colleague on the Vice Chancellor's Executive.¹

2.3 Requests for access without the employee's consent should be made using the form attached to this policy, and must include:

- Exactly what data is required.
- Exactly who will need access.
- The reason access is required, including the reason why the employee's consent has not been obtained.
- The time frame during which access to the data is required.

2.4 Requests should be as specific as possible about what data is required. For example by identifying specific document names, specific keywords, or date ranges when data was created or last modified. Requests that are overly broad will not normally be granted.

¹ Please check with Human Resources.
2.5 Requests for access should not be open ended. There must be an end date specified after which access will no longer be required. If additional time is needed, a second form should be submitted for approval.

2.6 Requests should be copied to the Information Security Manager, who will record them. It is recommended that requests be discussed with the Information Security Manager ahead of time to confirm that the requested access is technically possible.

2.7 Requests for access required in the course of an investigation into an employee should normally come from the HR partner who is managing the investigation.

2.8 When access is required as part of a legal obligation on the University, suitable approval must still be sought. In particular, requests by the police or other UK agencies with duties relating to the prevention and detection of crime, apprehension and prosecution of offenders, collection of tax or duty, or safeguarding national security must still get approval before access is given.

**Section 3: Exceptions**

3.1 Members of IT Services will, from time to time, need to access areas where employee’s individual data is stored, for the purposes of systems maintenance or the implementation of Information Security controls.

3.2 Such access must be authorized by an appropriate IT manager, and must be restricted only to the access required to complete the required tasks.

3.3 Requests to access the data of the University Secretary and Chief Compliance Officer without consent should be approved by the Vice Chancellor or Deputy Vice Chancellor instead.

3.4 Requests to access the data of the Information Security Manager without consent should be copied to the Associate Pro Vice Chancellor and CIO instead.

3.5 If there is an urgent requirement for access – for example where there is a clear and immediate risk of harm to a student or member of staff – temporary authorization may be given by any member of VCE except for the Associate Pro-Vice Chancellor and CIO. Formal authorisation from the University Secretary and Chief Compliance Officer should still be sought as soon as possible.

**Section 4: Accessing the data**

4.1 Once the request has been approved IT Services will arrange access.

4.2 Employees who have been given access must comply with the Data Protection policy and the Acceptable Use of Information Assets policy at all times. In particular, great care must be taken to only access the minimum amount of information required.

4.3 If employees who have been given access come across private data that is not related to the University, it should be ignored and not accessed. While reasonable personal use of University systems is allowed, employees are advised to separate personal and work data as much as possible in order to prevent inadvertent access by others.
Section 5: Relevant Legislation and other policies

Human Rights Act 1998


Data Protection Act 1998

Computer Misuse Act 1990
www.legislation.gov.uk/ukpga/1990/18/contents

Freedom of Information Act 2000
www.legislation.gov.uk/ukpga/2000/36/contents
Form U: Request to access User Data at UWL

SECTION 1: REQUESTER DETAILS To be completed by the person requesting access to data.

<table>
<thead>
<tr>
<th>1a) Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1b) Job title/function:</td>
</tr>
<tr>
<td>1c) School/Central Service Department:</td>
</tr>
<tr>
<td>1d) Telephone extension:</td>
</tr>
<tr>
<td>1e) Email address:</td>
</tr>
</tbody>
</table>

1f) Who will need access to the data?

☐ Tick this box if the requestor listed above requires access, and list any other employees who need access below.

1g) Will the data be passed on to a third party?

☐ Tick this box if data is to be passed to a third party, and identify them below.
**SECTION 2: DETAILS OF DATA**

Please try and give as much information as possible.

<table>
<thead>
<tr>
<th>2a) Whose data is access to be granted to?</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>If possible include their email address</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2b) What data is access to be granted to?</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Be as specific as possible and identify only the data you need. Example answer: Microsoft Word documents, stored in the user’s K: drive, modified in January 2018 and containing the phrase “John Smith”</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2c) Why is it necessary to grant access to this data?</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Include the reason consent has not been sought.</em></td>
</tr>
<tr>
<td><em>Example answer: Employee is on annual leave and we have not been able to contact them. We need to confirm the contents of a letter sent to student John Smith in January</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2d) How long will access to the data be required for?</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Open-ended requests will not usually be granted.</em></td>
</tr>
</tbody>
</table>
SECTION 4: AUTHORISATION

I am satisfied that access to this data is necessary, in accordance with UWL’s policies, and lawful.

<table>
<thead>
<tr>
<th>University Secretary &amp; Chief Compliance Officer (or other Executive Officer)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Signature | Print Name | Date

A copy of this signed and completed form should be returned to the Requester.
A copy should also be sent to the Information Security Manager
The original should be retained by the Compliance Officer until [..................^]

[^insert retention date]