Document Ownership and Control

This document is owned by the University’s IT security Co-ordinator. It is subject to change and version control and any amendments will be recorded below.

Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Circulation</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-0-0</td>
<td>20/04/2015</td>
<td>IT Website</td>
<td>First Formal Release</td>
</tr>
</tbody>
</table>

Version Awareness

The audience of this document should be aware that a printed copy may not be the latest available version. The latest version, which supersedes all previous versions, is available [here](#). Those to whom this document applies are responsible for familiarising themselves periodically with the latest version and for complying with its requirements at all times.
Introduction

1. OneDrive - University of Leeds (hereafter referred to as the Service) provides high-volume data storage and data sharing facilities and introduces flexible working practices by increasing accessibility to data through a variety of Internet-connected devices.

2. Whilst enabling this flexible working and increased accessibility the University has to ensure that the use of the Service by staff does not result in a security breach such as the leakage or disclosure of University data in contravention of the law, or in breach of contract, or the loss of intellectual property.

3. In order to prevent a security breach as a result of staff using the Service for business reasons, the Service may only be used for University data in full compliance with the Terms & Conditions set out below. Students’ use of the Service is not governed by these Terms & Conditions.

4. By using the Service for University data you commit to fully comply with these Terms & Conditions. Anyone who is found to be non-compliant with the requirements specified below, in relation to University data, may have the facility withdrawn and may face disciplinary action in accordance with existing University procedures.

What is OneDrive - University of Leeds?

5. The Service comprises a ‘cloud based’ 1 TB capacity data storage facility which:

   - Gives each member of staff a cloud storage area which they own as a user;
   - Enables users to create, store and edit documents using Microsoft Office Online, without having Microsoft Office on their computer;
   - Allows users to share access to and work on files collaboratively with colleagues both inside and outside the University;
   - Eliminates the need to use USB memory sticks, other removable media or manually copy data onto any mobile devices;
   - Provides the means for users to recover documents that have been deleted from the Service for at least 90 days; and,
   - Provide integrated version control, allowing previous versions of documents to be stored and accessed.

6. The Service can be used to store and access private (non-University) data as well as personal work-related data.

7. The Service is the only cloud based facility which is approved for the storage of University Classified information, but such information should only be stored for as long as necessary to achieve the immediate sharing requirement. Highly

* Although at the time of publication this is limited to 1 TB storage this is expected to increase to no defined limit in overall individual storage allowances in the future. No single file can exceed 2 GB in size (expected to be 10 GB shortly) and users can only synchronise 20,000 files to a device if they are using the Service app (see ‘How OneDrive - University of Leeds is used’ below).
Confidential information (as defined in the University’s Information Protection Policy) must only be stored in the Service if encrypted. Confidential and Highly Confidential information is defined at Annex A, along with examples of information falling within the respective categories. Further information on the use of cloud-based facilities for University data can be found here.

**What is OneDrive - University of Leeds used for?**

8. *The Service* can be used by the owner for creating, storing and sharing folders and individual documents. It is ideal for storing documents which are needed when staff are away from their computer, which can then be accessed using a web browser.

9. *The Service* can also be used with a OneDrive for Business ‘Sync App’ which allows the owner to make a local copy of all the data stored in the Service on a device. Before using the Sync App on any device the security controls in Paragraphs 30 and 31 must be in place.

10. *The Service* allows collaborative access to documents at individual and group level within and outside of the University.

11. It is important that users of the Service fully understand its purpose. It is not intended to be used as a:

- Replacement of your Home Directory (M: Drive) which is still the recommended location for the long-term storage of Highly Confidential information;
- Replacement for your University departmental file storage (N: Drive). The N: Drive is to be used for the storage of all shared school/departmental files;
- Document sharing facility. The owner of the Service can create a locally synced copy of those folders and documents. These folders and documents can be shared with other users who can also synchronise that content locally. Document and folder check-out is not possible, nor is the assignment of administrative permissions to users other than the owner of the Service. As a result, document sharing capabilities are limited;
- Place to install software; and,
- Place to store files used to run software or hold user settings required by software.

A comparison between the Service and the M: Drive can be found at Annex B.

**Using OneDrive - University of Leeds for Privately-Owned Data**

12. All use of the Service by individuals for storing and accessing private and personal data (i.e. that which is not associated with the University) falls outside the remit of these Terms & Conditions.

13. All such use of the Service is entirely at the risk of individuals and the University cannot be held accountable for the disclosure, loss or corruption of any privately-owned data.
14. Although the Service is fully managed and supported, the University cannot guarantee its full availability at all times and cannot commit to resolving any unavailability of service within any given timeframe.

How is OneDrive - University of Leeds used?
15. The Service can be used via a web browser after logging into https://office365.leeds.ac.uk or through the use of the OneDrive for Business Sync App.

Terms & Conditions of Use
16. All use of the Service for University data must be in full compliance with the University's Information Protection Policy at all times.

17. By using the Service for University data each participant is personally responsible and accountable for compliance with the University’s Information Security Policy and these Terms & Conditions of Use.

18. In accordance with the University’s Information Security Policy, Highly Confidential information must not be copied to or stored within the Service unless encrypted and then only for the shortest period necessary for business operations.

19. The downloading of University data to a device using the OneDrive for Business app is only permitted if the security controls specified at #30 and #31 are being fully met.

20. Access to Classified University data must be restricted to only University of Leeds employees and external collaborators who need access to it for operational purposes.

21. Where external collaborators are granted access to University data it must be kept to the minimum necessary for the purpose of the collaboration.

22. It is the responsibility of each user of the Service to ensure that an official University non-disclosure agreement / confidentiality undertaking is in place before allowing shared access to Classified University data when collaborating with external partners.

23. When working collaboratively with external parties it is the responsibility of each user of the Service to highlight any data which is University Classified and to ensure that the collaborator(s) understand the controls which they have to apply and can apply, as a condition of access, in order to protect that information before sharing is enabled.

24. It is the responsibility of each user of the Service to ensure that they comply fully with requirements of the Data Protection Act 1998 by adhering to the University’s Code of Practice on Data Protection. In doing so they are to ensure that they do not allow access to any personal information (as defined by the Act) to any

1 Please consult with the University Legal Advisors Office
person outside of the University\(^2\) or to anyone else who is not authorised to receive it.

25. Staff accessing the Service from computers or other devices in public areas must ensure that information they are viewing cannot be overlooked by those who are not entitled to view it.

26. Computers and portable devices must not be left unlocked and unattended whilst connected to the Service.

27. Staff using the Service for the storage of both private and University data are to keep the two data sets apart and clearly labelled.

28. Except in cases where staff are working collaboratively with people outside the University, no access to University data is to be granted to Non-University personnel.

29. Once staff cease University employment they are no longer entitled to retain or have access to official University data or the Service. Individuals are contractually obliged to delete any University data that they have access to unless they have permission to retain such data in accordance with the University's Data Retention Policy.

Security Controls

30. The following security controls must be active on all equipment which is used to access the Service:
   - PIN or password access control;
   - PIN or password protected timeout after a period of inactivity;

31. The following additional security controls must be active on portable equipment which is used to access the Service:
   - Data encryption;
   - Find my device; and,
   - Remote wipe.

32. Where available the device is to have anti-virus software installed which must be kept fully up to date.

33. Software on such devices is to be updated when updates become available and security patches are to be applied upon their release.

34. If you use a home or other non-University computer to create or access classified information, make sure that the computer has up-to-date security protection, and that it is password protected so that no-one else can use it to view University information.

35. The theft or loss of any device which is used to access the Service must be reported to the IT Service Desk at the first opportunity.

\(^2\) Collaborative research projects involving personal work-related data, where data subjects have consented to the research, are excluded from this requirement.
36. The University reserves the right, via a controlled and accountable process, to view all content of the Service without notifying the owner. Any personal or private information that the owner chooses to store within the Service should be placed within a folder structure which clearly identifies it as non-University information. The University will endeavour to protect privacy should it be necessary for systems administrators to access the Service.

37. The University reserves the right to withdraw rights of access and/or to delete the contents of the Service without notice. Wherever practical and reasonable the University will provide advanced notification of such action should this become necessary.

Sources of Help and Assistance

38. For help and advice using the Service please contact the IT Service Desk by email at itservicedesk@leeds.ac.uk or by telephone on (0113 34) 3333. Alternatively visit http://it.leeds.ac.uk/info/223/onedrive_university_of_leeds.
ANNEX A – Confidential and Highly Confidential Information

Confidential and Highly Confidential information is defined with the University’s Information Protection Policy as follows:

- **Confidential** applies to information disclosure of which to unauthorised recipients could have a *negative impact* on individuals or the University.
- **Highly confidential** applies to information disclosure of which to unauthorised recipients would be likely to result in *serious damage* to the interests of individuals or of the University.

Any information that is not categorised as either ‘Confidential’ or ‘Highly Confidential’ is 'unclassified'. No particular controls apply to the disclosure of unclassified material.

### Personal Information

<table>
<thead>
<tr>
<th>Unclassified</th>
<th>Confidential</th>
<th>Highly Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymised data[^3]</td>
<td>Individual’s passport details, home address and telephone number.</td>
<td>Financial information regarding individuals e.g. payment information (credit card details), bank account details, information about indebtedness (student fees).</td>
</tr>
<tr>
<td>Data agreed by data subjects to be put into the public domain.</td>
<td>Individual’s name plus home address/postcode, age and home telephone numbers.</td>
<td>Information on individual’s racial or ethnic origin, political opinion, religious or other beliefs, physical or mental health or criminal record.</td>
</tr>
<tr>
<td>Publicly available staff directories including work telephone numbers, e-mail address and Department information.</td>
<td>List of student names and their student ID number or list of staff names and their personnel number.</td>
<td>Attendance and academic progression information/disciplinary information relating to an existing University student.</td>
</tr>
<tr>
<td>Simple list of names with no other data.</td>
<td>Names and addresses of student applicants to the University.</td>
<td>Preliminary degree classification/transcript information pending formal approval and any publication.</td>
</tr>
<tr>
<td>Information on individuals available through social network sites where information provided on condition that will be public domain information.</td>
<td>Attendance details relating to an existing student.</td>
<td>References for students or staff[^4].</td>
</tr>
<tr>
<td>Final degree classification.</td>
<td>Student transcript</td>
<td></td>
</tr>
</tbody>
</table>

[^3]: For these purposes anonymised data is data which does not relate to a living individual and cannot identify an individual, or cannot identify an individual through other information which is in the possession of, or is likely to come into the possession of the organisation processing (see section 1 (1) (a) of the DPA 1998.

[^4]: Content dependent e.g. information relating to health, criminal record or disciplinary matters, would make the reference/UCAS form highly confidential.
### Non-Personal Information

<table>
<thead>
<tr>
<th>Non-Personal Information</th>
<th>Unclassified</th>
<th>Confidential</th>
<th>Highly confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information contained within an organisation's annual corporate report.</td>
<td>Research grant applications/proposals&lt;sup&gt;6&lt;/sup&gt;</td>
<td>Information relating to supply or procurement of goods/services prior to approved publication.</td>
<td></td>
</tr>
<tr>
<td>Information that can be obtained from publicly available directories or regulatory bodies e.g. Companies House or HEFCE.</td>
<td>Assessment material prior to “unseen” assessment</td>
<td>Future marketing or student fees information not yet agreed to be made public.</td>
<td>Other information that may be regarded as a trade secret or otherwise highly commercially sensitive.</td>
</tr>
<tr>
<td>Information contained within an organisation's web sites for public dissemination.</td>
<td></td>
<td>Information relating to restricted intellectual property rights or otherwise covered by a confidentiality agreement/contractual term.</td>
<td>Legal advice and other information relating to legal action against or by the University.</td>
</tr>
</tbody>
</table>

**Note.** The above are only indicative general examples of personal and non-personal information. As highlighted in the footnotes and main body of the [Information Protection Policy](#), the mix of information, the amount of information and the medium in which the information is held can change the classifications.

<sup>5</sup> Adding additional combinations of data can change the overall status. Simply increasing the volume of data can also change status.

<sup>6</sup> Content dependent e.g. information subject to imminent academic publication or industrial collaborators may lead to application/proposal being Highly Confidential.
## ANNEX B – Comparison of M drive with OneDrive - University of Leeds

Each member of staff at the University has a home directory (M: Drive). This area is provided for the storage of personal files and work files that are not required by other staff in the same school or department. Conversely, the file share area (N: Drive) is provided for the storage of all business-related files to which colleagues in your school or business may need access to.

The table below answers a few key questions about when you should use the Service and when you should use your M; Drive.

Please note that both the Service and the M: Drive are administered by, and may be accessed by, University of Leeds IT systems staff in order to maintain effective operations.

<table>
<thead>
<tr>
<th>M: Drive</th>
<th>OneDrive - University of Leeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the two file storage facilities?</td>
<td>File storage area hosted on University of Leeds servers and managed by University of Leeds staff.</td>
</tr>
<tr>
<td>What can the storage facilities be used to store?</td>
<td>Any data - Unclassified, Confidential and Highly Confidential data as defined in the Information Protection Policy</td>
</tr>
<tr>
<td>How much default storage is available?</td>
<td>DS Staff : 5 GB, Admin Staff : 2 GB</td>
</tr>
<tr>
<td>Are these storage facilities accessible through personal devices, using the wireless network or over the internet?</td>
<td>Yes, using the Desktop Anywhere service</td>
</tr>
<tr>
<td>Can these storage facilities be used to share files and folders with other people?</td>
<td>This is not a recommended or supported use of the service.</td>
</tr>
<tr>
<td>Can these facilities be used to make electronic work submissions to the</td>
<td>Yes, when using an on campus PC or from any device using Desktop Anywhere, the mapped</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VLE?</td>
<td>network 'M' drive can be used to make electronic submissions, either directly into the VLE or through Turnitin. Or by saving a local copy of the file to your device and then uploading it to the VLE.</td>
</tr>
<tr>
<td>Are these facilities available from on campus staff or cluster PCs?</td>
<td>Yes, after login to a PC this appears as a mapped drive, known as the “M” drive.</td>
</tr>
<tr>
<td>Are these facilities available from a web browser?</td>
<td>Yes, from a web browser after log in to the Office 365 service at <a href="https://office365.leeds.ac.uk">https://office365.leeds.ac.uk</a></td>
</tr>
<tr>
<td>Is recovery of previous file versions possible?</td>
<td>Yes, by reviewing restore points which are created once a day, you may be able to identify a previously saved file.</td>
</tr>
<tr>
<td>Is recovery of deleted files possible?</td>
<td>Yes, by reviewing restore points which are created once a day, you may be able to find files if they were saved before they were deleted.</td>
</tr>
<tr>
<td>Is FTP access available?</td>
<td>Yes, instructions on FTP access to your home directory are available <a href="#">here</a>.</td>
</tr>
<tr>
<td>Is FTP access available?</td>
<td>No, there is currently no support for FTP access to the Service.</td>
</tr>
</tbody>
</table>