Acceptable Use Statement – OneDrive

Version – v2 – April 2026

Policy Statement Author – IT Strategy & Governance Manager

Procedure Owner – Vice Principal (Finance and Infrastructure)

Parent Policy Statement – Information Technology Policy Statement

Public Access or Staff Only Access – Public

Version – Version 2 – April 2026

Changes and Reason for Changes –minor amendments, included to reflect UWS values.

Contents

1. Overview 3
2. Purpose 3
3. Scope 3
4. Introduction 3
5. Policy Statements 4
6. Best Practice 5
6.1 Use of USB Storage Devices 5
7. Compliance and Monitoring 6
8. Support and Training 6
9. How OneDrive supports UWS core values 6
10. Review and Revision 6
11. Feedback 6
APPENDICES 7
Appendix 1 – Glossary of Terms 7
Appendix 2 - Data Security Guidance for Staff 8

1. Overview

This document is an extension of the UWS Master Acceptable Use Policy (AUP), in that it specifically strengthens and deepens the policy statements in the master AUP. This AUP specifically details the policy statements that need to be in place in order for this service to be used, monitored, managed and controlled in an efficient and effective manner. Ensuring that this service is conformant and/or compliant with UWS adopted standards, frameworks, patterns and guidelines as well as those of the UWS.

This document is the UWS Acceptable Use Statement (AUS) for Microsoft OneDrive. It provides the core set of security principles and expectations on the acceptable use of MS OneDrive.

2. Purpose

This policy outlines the acceptable use of OneDrive for saving files within the UWS environment. It aims to ensure the security, integrity and accountability of sensitive data and to provide guidelines for appropriate usage by University colleagues.

The Statement aims to protect all users of UWS equipment and data, as well as minimising the risks associated with their use by providing clarity on the behaviours expected and required by UWS employees, Agents, Service Providers, Contractors, and Consultants. It sets a framework on how the UWS services and systems should be used to meet legal, contractual, and regulatory requirements and defines how individuals must behave in order to comply with this AUS.

To ensure that individuals understand their responsibilities for the appropriate use of UWS resources, systems and services. Understanding what is expected will help individuals to protect themselves, colleagues and UWS equipment, information and reputation and ensure that there is clear accountability.

3. Scope

This policy applies to:

- UWS M365 Tenant
- UWS employees, students, third-parties, third-party associates and UWS partner organisations and agencies.

4. Introduction

UWS accepts that use of Microsoft OneDrive is essential to enabling UWS to meet its aims and objectives. It is a requirement that your use of this software is legal and appropriate for delivering the requirements of your role without creating unnecessary risk.

This document should be read in conjunction with the following: Information Management and Data Protection Policies, in particular;

- Data Classification and Handling Policy
- IT Acceptable Use Statement
- Guidelines for Use of Social Media at UWS
- IT Password Management Procedure

You are also bound by any relevant legislation, such as Data Protection and Copyright laws and the information below.

Misuse of the service can be investigated and lead to disciplinary action. The UWS reserves the right to monitor use and compliance with the law and policy; we may use system analytics to achieve this.

5. Policy Statements

Policy ID **AUP.UWSMS1DRIVE.001**	**Statement**
001.	All Users shall be made aware of the Acceptable Use Statement – OneDrive (this document) and, where appropriate, provided with security awareness training which covers this statement.
002.	Outside of proprietary systems e.g. Pure, Banner, iTrent etc. Microsoft OneDrive, SharePoint and Teams are the only approved cloud storage locations for storing and sharingM365 files within the UWS environment. Personal data stored in proprietary systems e.g. Banner, iTrent should not be downloaded and stored on other storage location without Legal/IT approval. No other cloud storage providers are permitted to be used for storing university-related files.
003.	Files and folders must not have names that are considered to be offensive or derogatory.
004.	Staff members are expected to comply with this policy and to use OneDrive responsibly. The university reserves the right to monitor OneDrive usage to ensure compliance with this AUS.
005.	The Documents Owner is automatically considered to be the Information Asset Owner (IAO) – along with having the responsibilities of this role.
006.	The IAO is responsible for ensuring documents are correctly classified, in accordance with the Data Handling and Classification Protocol
007.	All files categorised as confidential must be password protected to ensure their security. If password protected, they can be stored on OneDrive. Where there is a requirement to share files with internal or external colleagues or partners, a

Policy ID AUP.UWSMS1DRIVE.001	Statement
	Secure Team should be used. Contact the IT Service Desk to request the configuration of a secure team.
008.	MS OneDrive must not be used to download, process, create, store and/or transmit any form of language, graphics/images and/or material that could be offensive or derogatory.
009.	OneDrive data is retained for 3 months after UWS user account deletion.
0010.	OneDrive owners are fully accountable and responsible in ensuring their documents and this service is used in an appropriate and relevant manner.
0011.	All users are responsible for ensuring that MS OneDrive usage is compliant with this AUS and other relevant supporting policies.
0012.	All users are responsible for ensuring that their activities and actions are compliant with this AUS and other relevant supporting governance documents.

Commented [RK1]: Add brief definition of what a Secure Team is and when it should be used

Commented [RK2]: Maybe define owner earlier in the document

Commented [RK3]: Changed assuring to ensuring

6. Best Practice

6.1 Use of USB Storage Devices

- The use of USB storage devices is strongly discouraged except in exceptional circumstances where it is absolutely necessary and must not be used as a long term storage solution. Data labelled confidential should never be saved to a USB device.
- Any USB storage devices used must be encrypted to protect the data stored on them.

Commented [RK4]: Add: "USB devices must not be used for long-term storage of university data."

Examples of exceptional circumstances where the use of USB storage devices might be necessary:

- **Offline Access**: When staff members need to access important files in locations without internet connectivity, such as during fieldwork or travel.
- **Data Recovery**: In situations where OneDrive is temporarily unavailable due to maintenance or technical issues, and critical files need to be accessed urgently.
- **Secure Backups**: For creating secure backups of important data that need to be stored in a separate location for disaster recovery purposes.
- **Special Projects**: When collaborating with external partners who do not have access to OneDrive, and secure file transfer is required.
- In these cases, it's essential that the USB storage devices used are encrypted to ensure data security and comply with the university's policies.

7. Compliance and Monitoring

- Staff members are expected to comply with this AUS and to use OneDrive responsibly.
- The university reserves the right to monitor OneDrive usage to ensure compliance with this policy. Any monitoring will be carried out only for specified and legitimate purposes, supported by an appropriate UK General Data Protection Regulation (UK GDPR) lawful basis such as compliance with legal obligations or the performance of tasks in the public interest. Audit logs may be reviewed where necessary, and all monitoring activities will be limited strictly to what is required to achieve these purposes.
- Any violations of this AUS may result referral to University disciplinary processes.

8. Support and Training

- The University will provide training and support for staff members on the proper use of OneDrive, Teams and general data security best practices.

9. How OneDrive supports UWS core values

- OneDrive Teams promotes **integrity** by providing a secure environment where files can be created and edited in manner that can be tracked and rolled back through versioning. Protecting data from change.
- By protecting users' files through access controls and allowing rollback OneDrive shows the respect that UWS has for users' data.
- OneDrive encourage s inclusivity by offering features such as Dictate, Immersive reader, Accessibility checker among others, these tools help users with disabilities write documents, chat, and share ideas in a way that works
- OneDrive upholds accountability through a combination of data protection measures, compliance with regulations, and robust incident response protocols.

10. Review and Revision

- This policy will be reviewed annually and updated as necessary to ensure it remains effective and relevant.

11. Feedback

- For any questions or concerns regarding this policy, staff members should contact IT.
    - TOPdesk Self Service Portal
    - helpdesk@uws.ac.uk

Commented [SM5]: This topdesk link doesn't work

APPENDICES

Appendix 1 – Glossary of Terms

Term	Description
AUP	Acceptable Use Policy
AUS	Acceptable Use Statement
IAO	Information Asset Owner
UWS	University of the West of Scotland
UK GDPR	UK General Data Protection Regulation

Appendix 2 - Data Security Guidance for Staff

Poor data security can lead to numerous serious risks for both individuals and the university. Here are some of the key risks:

1. Data Breach

- Unauthorised access to sensitive data can result in data breaches, exposing personal, financial, and confidential information to malicious actors.

2. Financial Loss

- Data breaches and cyberattacks can lead to significant financial losses due to theft, fraud, ransom payments, and the costs associated with mitigating and recovering from the breach.

3. Reputation Damage

- Organisations that suffer data breaches may experience reputational damage, losing the trust of customers, partners, and stakeholders.

4. Legal and Regulatory Penalties

- Non-compliance with data protection regulations (such as UK GDPR) can result in large fines and legal penalties for organisations that fail to adequately protect data.

5. Operational Disruption

- Cyberattacks and data breaches can disrupt business operations, leading to downtime, loss of productivity, and potential loss of business opportunities.

6. Identity Theft

- Poor data security can expose individuals to identity theft, where attackers use stolen personal information to commit fraud or other malicious activities.

7. Intellectual Property Theft

- Inadequate data security can result in the theft of intellectual property, such as trade secrets, proprietary information and research and development data.

8. Loss of Customer Trust

- Customers may lose trust in an organisation that fails to protect their data, leading to decreased customer loyalty and potential loss of business.

9. Cyber Espionage

- Poor data security can make organisations vulnerable to cyber espionage, where attackers steal sensitive information for political or economic gain.

10. Human Error

- Lack of proper training and awareness can lead to human error, such as accidental data leaks, misconfigurations, or falling victim to phishing attacks.

By understanding and addressing these risks, organisations can implement robust data security measures to protect sensitive information and maintain the trust of their stakeholders.