# Acceptable Use Statement - OneDrive

Version – v1 – February 2025

**Policy Statement Author** – IT Security and Customer Support Manager

**Procedure Owner** – Vice Principal (Finance and Infrastructure)

**Parent Policy Statement** – Information Services Policy Statement

**Public Access or Staff Only Access** – Public

**Version** – Version 1 – February 2025

**Changes and Reason for Changes** – new statement.

## Contents

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

## 1. Overview

This document is an extension of the UWS Master IT Acceptable Use Statement, in that it specifically strengthens and deepens the policy statements in the master AUS. This AUS specifically details the policy statements that need to be in place in order for this service to be used, monitored, managed and controlled in and 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 MS OneDrive. It provides the core set of security principles and expectations on the acceptable use of MS OneDrive.

## 2. Purpose

This statement outlines the acceptable use of OneDrive for saving files within the UWS environment. It aims to ensure the security and integrity 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 in order 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 statement 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 UWS's responsibilities does not create unnecessary risk.

Microsoft Teams enables you and your colleagues to send instant messages, make video calls and keep up to date with your teams. Over time we will be adding more functionality allowing you to better collaborate, share and edit files as a Team and with external partners where appropriate. For now, you should use Teams as you would Jabber and WebEx.

Because Teams allows for greater interaction between UWS employees, UWS must ensure that it is used appropriately and responsibly. This usage statement sets out how to do this, makes staff aware of how Sites should be managed and how new Sites can be requested. It should be read in conjunction with the following:

- Dignity and Respect at Work Guidelines Employees
- IT, Information Management and Data Protection Policies, in particular;

- Information Security Procedure
- IT Acceptable Use Statement
- Copyright Guidance
- IT Password Management Procedure
- Data Protection Code of Practice
- IT Software and Licencing Control Statement
- Guidelines for the Use of Social Media for UWS Staff
- Data Handling and Classification Protocol

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**<br>**AUP.UWSMS1DRIVE.001** | **Statement** |
|---|---|
| 001. | All Users shall be made aware of the Acceptable Use Statement (this document) and, where appropriate, provided with security awareness training which covers this statement.. |
| 002. | Microsoft OneDrive and Teams are the only approved cloud storage provider for storing and sharing files within the UWS environment.<br>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. | Sensitive files, including but not limited to personal, financial, or confidential information can be stored on OneDrive. |
| 005. | Staff members are expected to comply with this statement and to use OneDrive responsibly.<br>The University reserves the right to monitor OneDrive usage to ensure compliance with this statement. |
| 006. | The Documents Owner is automatically considered to be the Information Asset Owner (IAO) – along with having the responsibilities of this role. |
| 007. | The IAO is responsible for ensuring documents are correctly classified, in accordance with the Data Handling and Classification Protocol |
| 008. | All files categorised as sensitive must be password protected to ensure their security. Where there is a requirement to |

| Policy ID<br>AUP.UWSMS1DRIVE.001 | Statement |
|---|---|
|  | share files with internal or external colleagues or partners, a Secure Team should be used. Contact the IT Service Desk to request the configuration of a secure team. |
| 009. | 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. |
| 0010. | OneDrive data is retained for 3 months after UWS user account deletion. |
| 0011. | OneDrive owners are fully accountable and responsible in ensuring their documents and this service is used in an appropriate and relevant manner. |
| 0012. | All users are responsible for ensuring that MS OneDrive usage is compliant with this AUP and other relevant supporting policies. |
| 0013. | All users are responsible for assuring that their activities and actions are compliant with this AUS and other relevant supporting governance documents. |

## 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.
- Any USB storage devices used must be encrypted to protect the data stored on them.

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 statement and to use OneDrive responsibly.
- The University reserves the right to monitor OneDrive usage to ensure compliance with this statement.
- Any violations of this statement may result in disciplinary action, following UWS 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. Review and Revision

- This statement will be reviewed periodically and updated as necessary to ensure it remains effective and relevant but no less frequently than every 2 years.

## 10. Feedback

- For any questions or concerns regarding this statement, staff members should contact IT Services.
    - uws.topdesk.net
    - helpdesk@uws.ac.uk

# 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 |
| FOI | Freedom Of Information |

## 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 GDPR or CCPA) can result in hefty 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.