

Internet Usage policy

Purpose

This policy sets out the acceptable use of the internet and online services at U3AC. It applies to all staff, volunteers, trustees, members and contractors using U3AC-provided internet access, irrespective of a person is using equipment owned by U3AC or equipment owned personally by them or a third party.

This policy should be read in conjunction with U3AC's other policies, particularly its Privacy policy, Social Media policy and its Communications policy.

General Principles

It is recognised that staff, trustees and volunteers will make use of the internet and online services when acting on behalf of U3AC. Everyone is responsible for ensuring that their use of such digital tools supports U3AC's values and is consistent with its statutory obligations.

Office staff are allowed to access the internet at work for limited personal use provided it does not interfere with their duties, does not incur cost to the organisation and does not breach this or any other U3AC policy.

Acceptable Use

All use of online systems must comply with the UK GDPR and the Data Protection Act 2018. In addition, appropriate use by staff will include:

- Research, communication, and online tools related to U3AC's activities.
- Accessing educational materials, training, and professional resources.
- Using organisational communication platforms (e.g., email or Google Meet).

Prohibited Use

The following is a non-exhaustive list of uses that are prohibited:

Any activity that is or may be illegal or unethical. This includes:

- Downloading, sharing, or accessing copyrighted material without permission.
- Engaging in harassment, bullying, discrimination, or hate speech.
- Accessing or sharing extremist, violent, or inappropriate content.
- Engaging in fraud, misrepresentation, or activities harmful to U3AC

The installation of unauthorised software or browser extensions, any attempt to circumvent security controls, firewalls, or filtering systems, accessing websites known to have malware or suspicious content, sharing passwords, login credentials, or secure access methods.

Excessive personal browsing or social media use during working hours. This includes:

- Online gaming, gambling, or streaming non-educational entertainment content.
- Using U3AC's internet for commercial, political, or fundraising activities not affiliated with the organisation.

Any use that could put a U3AC member at risk or breach U3AC's safeguarding principles.

Monitoring

U3AC reserves the right to monitor and log internet activity. However, monitoring will not be excessive and will be limited to what is necessary to ensure security, prevent misuse, and comply with legal obligations. Individuals may request details of what monitoring occurs.

Security

Passwords for email accounts, membership systems, and online platforms must be strong, confidential, and changed promptly if there is reason to believe that they have been compromised. Personal data must only be stored or shared using approved, secure methods. Devices used for U3AC work should have up-to-date antivirus protection and security updates. Any suspected data breach must be reported at once to the Operations Manager, the Chair or Secretary, who in turn will report the matter promptly to the full Council.

Where personal devices are used for U3AC work, users must ensure the device is password-protected, kept updated, and not shared with others when logged into U3AC systems.

Approved by Council: 1 May 2026

Next review date: May 2028