3. Scope

Usage of UIAs, including but not limited to:

- End-user computers.
- Physical and virtual servers.
- Mobile devices including phones and tablets.
- Network devices and supporting services.
- Hosted or cloud-based services.
- Network and Internet based exchange of information.
- Remote access.
- Printed media.

4. Policy

For all usage of UIAs, the following acceptable use principles will be followed:

4.1. General principles

4.1.1. Users confirm that prior to use of UIAs, that they agree to this Acceptable Use Policy (AUP) and understand that breaching this policy may result in disciplinary procedures.

4.1.2. Users may only use UIAs for lawful activities and must never threaten the University's reputation, bring the University into disrepute, or jeopardise the integrity or security of UIAs.

4.1.3. Users must not try (directly or indirectly) to get more access to UIAs beyond their approved rights and permissions.

4.1.4. Users must not perform any activity that prevents legitimate access to UIAs.

4.1.5. Users must act responsibly and professionally, and not engage in any behaviours considered: abusive, offensive, bullying, defamatory, obscene, pornographic, homophobic, blasphemous, seditious, racist, discriminatory, or harassing.

4.1.6. Users must report any breach of this policy by emailing ccsshelp@mdx.ac.uk

4.1.7. Users must familiarise themselves with the University's Information Security and Awareness materials.

4.1.8. Except where the University cannot exclude or limit its liability as a matter of law, the University shall have no liability to any Users in connection with the non-availability of the University's computing facilities howsoever arising, including in negligence.

4.2. User IDs and passwords

4.2.1. Access to UIAs is based on unique IDs or other forms of credentials such as digital certificates. Users must not share their ID with anyone else. Each User is accountable their actions.

4.2.2. Users must not share their passwords or any other authentication mechanisms such as multi-factor physical and software tokens (electronically, physically, or verbally).

4.2.3. Authorised personnel may access Users' accounts where the owner has given their explicit approval and with valid reason. For business continuity, HR may approve such access where the owner is unable to.

4.3. Managing and protecting information

4.3.1. Only approved University devices and services should store, process and/or send UIAs.

4.3.1.1. Where staff may need to store, process, or send UIAs on personal devices, these devices must meet Cyber Essentials requirements.

4.3.1.2. Users must remove UIAs

4.3.2. Users must not share or contract services that store, process, or send UIAs without explicit and documented permission.

4.3.3. Users confirm that they and the University have a legal responsibility to protect personal and sensitive information.

4.4. Personal use of UIAs

4.4.1. Users confirm that they are personally accountable for what they do online whilst using University services and technologies or acting on behalf of the University.

4.4.2. Commercial use of UIAs is prohibited without explicit and documented permission.

4.4.3. Use of essay mills and buying assignments are prohibited.

4.4.4. The University provides UIAs to aid with day-to-day work, however, limited personal and recreational use is allowed.

4.5. Electronic and voice communication

4.5.1. Users must not send unsolicited bulk email messages, chain mail or spam.

4.5.2. Users must act responsibly and appropriately when using UIAs to communicate internally and externally.

4.5.3. Users must be vigilant to phishing emails and know how to spot and report them.

4.5.4. Staff should not forward their emails to personal mailboxes withou5.9 (eat) (nal)2.4.2 (

Users must forward them.

- Janet Acceptable Use Policy
- Applicable compliance guidance

7. Further Information

- Cyber Security Guidance for Students
- Digital Wellbeing Guidance for Staff
- Cyber Security Awareness Course for Staff

In accordance with relevant Regulations, any transgression or breach of the above restrictions or policies will be deemed as gross misconduct and/or a serious offence which may result in withdrawal of services and/or expulsion following a proper hearing of the case. Users will be held responsible for any claims brought against the University in respect of any legal action to which the University is, or might be, exposed because of User's misuse of UIAs, including reimbursing the University for any financial liability which the University suffers because of a User's actions or omissions. The University will not hesitate to follow its Investigations Procedure and if necessary, contact the police if it discovers unlawful use of UIAs.

The University has a statutory duty under Section 26(1) of the Counter-Terrorism and Security Act 2015 ("the Act") when exercising its functions, to have due regard to the need to prevent people from being drawn into terrorism. The University may impose filtering and/or monitoring, as required in its view, to support this duty.

Users will be held responsible for any claims brought against the University for any legal action to which the University is, or might be, exposed because of User's misuse of UIAs including reimbursing the University for any financial liability which the University suffers because of Users actions or omissions.

8. Version Control

The most current version of this controlled document is stored in our document management system (DMS). Authorised reviewers are required to 'check out' documents and summarise any changes