Acceptable Use Policy

Version:	1.0
Last Review Date:	16/04/2021
Last Reviewed By:	Terry Sullivan
Document Owner:	Paula Vickers
Approver:	Sophie Bowen
Document Status:	Approved

1. Rationale

To protect University Information Assets (UIAs[1]) through the definition of acceptable user interactions, thereby reducing potential impacts to confidentiality, integrity, and availability.

This policy explains how:

- authorised: staff, students (applicants, current and alumni) and third parties (collectively referred to "Users") may use UIAs.
- Users or the University may be liable in law for misuse of UIAs and the consequences if the rules and regulations set out in this policy are not followed.
- to protect UIAs through the definition of acceptable user interactions that reduce any potential impacts to confidentiality, integrity, and availability.

This policy applies wherever and however UIAs are accessed, irrespective of device location or ownership, e.g., from the University's premises, via the Internet; University owned or personally owned.

The University encourages all Users to use UIAs as tools to assist their work; Users have no automatic right to use the facilities for any other purpose. UIAs may only be used in accordance with this policy.

The University reserves the right to amend this policy at any time and will notify all Users of any changes it makes.

The University considers failure or refusal to comply with this policy to be a serious disciplinary offence which may lead to actions including withdrawal of services, and/or dismissal/expulsion without notice in accordance with:

- The User's contract of employment (or work order) with the University, the 'University Grievance & Disciplinary Procedures' and the 'Staff Handbook' (together, the "Staff Regulations") – specific to staff and third parties, or
- the University's Regulations specific to students.

Accordingly, this policy is not a definitive statement of the purposes for which UIAs should or should not be used, and the University reserves the right to apply this policy in a purposeful manner.

2. Purpose

Defined user guidance to ensure that usage considers:

- University authorised processes, methods, and software to protect UIAs during normal use or operation.

[1] UIAs are defined as any asset (or people) that store, transmit or process University information.

- Preventing interactions with UIAs that may breach legal, contractual, or regulatory requirements.

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 from personal devices prior to disposal.
4.3.1.3. The University accepts no responsibility for personal data stored on devices or storage facilities.
4.3.1.4. Users must remove or transfer UIAs when no longer authorised.
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 without University approval.
4.5.5. Users must not try to assume the identity of another user, or create, send, or change material designed to mislead people about who originated, authored, or authorised it.

4.6. Appropriate Internet use

4.6.1. Users must not, other than for ethically cleared, properly approved and lawful research purposes, visit, view, store, download, send, display, print or distribute any material relating to:
4.6.1.1. Sex or pornography.
4.6.1.2. Lewd or obscene material of any nature or other material which may be likely to cause offence to another person.
4.6.1.3. Terrorism or cults.
4.6.1.4. Hate sites (racial or other).
4.6.2. Users must not harm the University's reputation, nor misrepresent the University's views or opinions through any Internet published materials and communications.
4.6.3. Users must be aware that their social media content may be available for anyone to see, indexed by search engines and archived for posterity.

4.7. Devices, systems, and networks

4.7.1. Users must not change any physical aspect (or the connectivity) of UIAs or attached equipment without authorisation.
4.7.2. For Internet connectivity on campus, Users must only connect personal devices to MDXOpen.

4.8. Physical security

4.8.1. Users must secure unattended UIAs through software controls or physical mechanisms.

4.9. Applicable compliance guidance

4.9.1. Users must respect copyright, licensing, and intellectual property.
4.9.2. Users must not download, install, or distribute unauthorised software.

4.9.3. As per applicable regulations, Users may face sanctions that include dismissal, expulsion, termination of contract, or be at risk of civil or criminal liability.
4.9.4. Users' usage and generated information (including emails) may be watched, filtered, changed, removed, or shown to meet legal, contractual, or regulatory requirements.
4.9.5. The University and Users must abide by all legal, contractual, and regulatory requirements or restrictions including but not limited to:
4.9.5.1. UK Data Protection Act 2018
4.9.5.2. General Data Protection Regulation (GDPR)
4.9.5.3. Freedom of Information Act 2000
4.9.5.4. Counter-Terrorism and Security Act 2015
4.9.5.5. Copyright, Designs and Patent Act 1988
4.9.5.6. Computer Misuse Act 1990
4.9.5.7. Communications Act 2003
4.9.5.8. Equality Act 2010
4.9.5.9. Racial and Religious Hatred Act 2006
4.9.5.10. Malicious Communications Act 1988
4.9.5.11. Investigatory Powers Act 2016
4.9.5.12. Privacy and Electronic Communications Regulations 2003
4.9.5.13. Payment Card Industry Data Security Standard (PCI DSS)

Exceptions
Users seeking an exception to acceptable use for ethically cleared, properly approved and/or lawful research purposes must obtain prior written approval from their Line Manager, Dean of School, or an appropriate member of the Executive. This approval needs to be reconfirmed in writing every 6 months.

5. Responsibilities

CCSS	• Definition of acceptable University software and devices approved for use. • Monitoring and provision of applicable technical controls that enforce acceptable use.
Authorised Reviewer	• Review this document, summarise any resulting changes and improvements, and create minor revisions.
Document Owner	• Maintain this document. • Assure the quality of any changes. • Create major revisions following document approval.
Approver	• Understand the organisational implications of this document and support its contents.

6. Compliance
The Acceptable Use Policy shall be enforced to meet specific compliance requirements, including but not limited to:

- Cyber Essentials
- UK Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- PCI DSS
- University Regulations
- University Grievance Procedure
- Disciplinary Procedure

- Academic Staff Handbook
- University Ethics Framework
- University Policies, Procedures and Guidance
- Microsoft Terms of Use
- 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 before 'check in'. Authorised reviewers may create minor revisions, e.g., 1.0 to 1.1.

Following approval, controlled documents are incremented to the next major revision, e.g., 1.1 to 2.0. As such, controlled documents with minor revisions have not been approved. Full version history is available within our DMS.