UNIVERSITY ACADEMY 92

MANCHESTER

IT Usage Policy

Implementation date:	**January 2021**
Version number:	**1.0**

Document type		Strategy
	✓	Policy
		Regulations
		Procedure
		Code of Practice
		Guidance
Area of UA92 business		Governance & Compliance
		Student Affairs
		Academic
	✓	People & Operations
		External Affairs
		Other
Document Name:	IT Usage Policy	
Author:	Digital Services and Innovation Manager	
Owner (if different from above):		
Document control information:		
Version number:	1.0	
Date approved:		
Approved by:		
Implementation date:		
Review due:		
Document location:		
Consultation required:		
Equality & Diversity		
Legal considerations (including Consumer Rights)		
Information Governance		
Students		
Employee Engagement Forum		
External		

REVISION HISTORY			
Version	**Date**	**Revision description/Summary of changes**	**Author**

CONTENTS

1. PURPOSE

1.1. The purpose of this document is to outline the responsibilities of Staff, Students and Partners when using UA92 IT infrastructure, equipment and systems.

1.2. Appropriate use of IT resources is crucial to protecting the institution and its community from harm caused by loss of data, identity theft and other digital and physical threats.

1.3. It is the responsibility of each member of the community to understand this policy and use their IT equipment, systems and resources in line with its principles

1.4. Any further guidance or training needed should be discussed with the person's line manager, coach or the Digital Services and Innovation Manager.

2. SCOPE

2.1. This policy applies to all employees, students, and partners at UA92, including visiting lecturers, board members and guests/guest speakers.

2.2. The oversight and control of this policy rests with Digital Services, in consultation with key partners and stakeholders.

2.3. Any breaches in this policy may be dealt with in line with the code of conduct applicable to either students or colleagues.

3. POLICY STATEMENTS

3.1. Acceptable Use

3.1.1. All use of IT equipment and systems should be in line with supporting the mission and goals of UA92 and conducted in a safe and responsible way.

3.1.2. All IT equipment and infrastructure remain the property of UA92 and can be monitored, reviewed, and disclosed to support its appropriate use.

3.1.3. Devices and Software should not be altered, installed, or otherwise modified unless authorised by Digital Services.

3.1.4. All interaction via email, Teams and other digital means should be used responsibly and in line with the UA92's values as outlined in the Ethics Framework, social media policy and the code of conduct applicable to your role.

3.2. Data Protection

3.2.1. All data and sensitive information should be stored securely and protected from unauthorised access and loss.

3.2.2. Passwords and accounts need to be kept secret and meet good standards of security, for example meeting minimum length requirements

3.2.3. Data and files are stored in only two places: Microsoft Teams and OneDrive.

3.2.4. Teams is for shared documents and collaboration, OneDrive for limiting access to yourself.
3.2.5. USB external drives are not to be used, only UA92 based cloud storage used as outlined above.
3.2.6. Files and data should only be shared when needed and only shared with those that need it, via Teams or OneDrive link
3.2.7. For further guidance on Data Protection see the GDPR and the Data Protection and Information Security Policy.
3.2.8. Files and data should not be downloaded from Microsoft Teams or SharePoint and stored locally on a USB or on devices.

3.3. Devices and Equipment

3.3.1. Devices and equipment issued by the institution remain the property of the institution and should be protected from loss and damage
3.3.2. Any defect or damage to any equipment should be reported to Digital Services as soon as possible and repair only attempted by authorised personnel
3.3.3. Equipment owned by UA92 should only be used for work associated with supporting the UA92's goals, and not for personal use.
3.3.4. Where devices have been issued, only those devices should be used for UA92 work and not personal devices
3.3.5. Where devices have not been issued to staff members, any personal devices used for UA92 work should be treated in the same way and kept secure. UA92 reserves the right to audit any device used for UA92 work purposes.
3.3.6. Devices need to be kept securely when not in use, and not shared with other members of the UA92 community or third parties.

3.4. Remote Working

3.4.1. When working or studying from home, you should ensure that the working environment is suitable to keep you safe, both digitally and physically.
3.4.2. WIFI networks should be secure and private, never use open WIFI such as coffee shops or bars.
3.4.3. Chargers, plugs, and other electrical components should be checked regularly and be in good working order, for example with no bent, exposed, or frayed wires. Only use chargers issued with your device.

3.5. Social Media

3.5.1. Please refer to the Social Media Policy applicable to your role: The Student Code of Behaviour for Students and the Social Media Policy for Staff.

3.6. Use of Personal Email Addresses

3.6.1. Personal email addresses are not to be used for work purposes.

3.7. Monitoring

3.7.1. UA92 reserves the right to regularly audit User activity and IT systems to ensure compliance with this and other UA92 policy.

3.7.2. Access to Company IT systems is provided on condition that users consent to monitoring in accordance with Policy.

3.7.3. Your use of Company IT systems constitutes your consent to the monitoring.

3.8. Access to personal information (staff, students, applicants, enquirers, third parties)

3.8.1. In the course of your role, you may have access to the personal information relating to students, applicants, enquirers, staff, the business of UA92 or third parties. You must comply at all times with the following when accessing systems that contain personal or confidential information:

i. Only process personal information in so far as required in order to complete the specific task related to UA92 business and not for any other reason.

ii. Do not reveal or disclose personal, sensitive or identifiable information to anyone other than the individual for the purpose of your job role.

iii. Do not download any individual's personal information onto personal devices such as USB sticks, phones, cameras etc., nor take any photo of any individual without their express permission.

iv. Safeguard and protect all personal information from unauthorised or unlawful processing, including (but not limited to) accidental loss, destruction or damage.

v. Inform the UA92 DPO immediately if you have done something (or are asked to do something) infringing the requirements of this Policy even where such action or breach is accidental or inadvertent.

vi. If you have any doubts about the confidentiality of any information, it must be regarded as confidential unless you are advised otherwise by your line manager.

4.0. **Related documentation:** detail any 'policies' which relate to this 'policy'.

4.1. GDPR and Information Security Policy

4.2. Student Terms and Conditions

4.2.1. https://ua92.ac.uk/student-regulations-policies

4.3. Colleague Accountability Statement and Ethics Framework

4.4. Student Code of Behaviour and Disciplinary Regulations

4.4.1. https://ua92.ac.uk/storage/app/media/UA92%20Student%20Disciplinary%20Policy%20Final.pdf

4.5. Social Media Policy