UCQ UNIVERSITY CENTRE QUAYSIDE

Safe Use of IT Policy

Version: 2
Revision date: 19/01/2021

Due for review: 19/01/2023

Table of Contents

1. Introduction

1.1 University Centre Quayside (UCQ) fully recognise their responsibilities to safeguard all students and is committed to providing a safe environment for study and work, including a safe online environment. UCQ will do all that it can to support its students and staff to stay safe online and to satisfy its wider duty of care. This policy encompasses both online safety and acceptable use of IT.

1.2 Staying safe online is defined for the purpose of this document as the process of limiting the risks to children, young people and vulnerable adults when using internet, digital and mobile technologies through a combined approach of policies and procedures, infrastructure and education. The breadth of issues within online safety is considerable, but can be categorised into three main areas of risk:

1.2.1 Content – being exposed to illegal, inappropriate or potentially harmful material such as exposure to age-inappropriate material, illegal or extremist content and misinformation

1.2.2 Contact – being subjected to harmful online interaction with other users such as grooming, radicalisation, fraud, scams and/or cyberbullying

1.2.3 Conduct – personal online behaviour that increases the likelihood of, or causes, harm such as sharing personal information, sharing location and addiction

1.3 Where required, laptops or tablets are provided and maintained for the benefit of all students. Students are encouraged to use and enjoy these resources and to ensure that they remain available to all. Any damage, malicious alteration or inappropriate use of the computer equipment may harm their education and that of other students.

1.4 To protect all in its care, UCQ must insist that all students adhere to its rules for the acceptable use of IT equipment.

2. Online safety

2.1 Digital skills are an essential skill for life and employment; ICT presents both risks and benefits to its users. The use of technology has become a significant component of many safeguarding issues including exploitation, radicalisation and abuse. Risks can arise from various ICT platforms, below is a non-exhaustive list of different platforms and their associated risks.

2.1.1 Use of internet technologies on any device. Risks associated with accessing inappropriate or illegal content, online fraud and scams, grooming and radicalisation, malware and viruses or online gambling sites.

2.1.2 Social media and messaging platforms. Risks associated with sharing personal information and damaging their digital footprint, location sharing, privacy settings, cyberbullying, trolling and online negativity and abuse, the sharing of “fake news” (disinformation and misinformation), grooming, radicalisation and “catfishing”.

2.1.3 Online gaming on multiple platforms including mobile apps, consoles, computers, social media, VR and TV. Risks associated with harmful addictions, grooming, radicalisation, age-inappropriate content, in-game purchases, privacy settings, links to gambling such as “loot boxes”.

2.1.4 Livestreaming services on multiple social media platforms including YouTube. Risks associated with sharing personal information, damaging digital footprint, location sharing and lack of control of content sharing.

2.1.5 Use of mobile phones text messaging services. Risks associated with bullying and harassment, grooming, sexting, sharing indecent images and ‘county lines’.

2.1.6 Use of email. Risks associated with bullying and harassment, phishing and spoofing.

2.2 UCQ has a number of measures in place to safeguard students and staff. These include:

2.2.1 UCQ ICT facilities and networks are safe and secure, with up-to-date security measures and software in place. The necessary filters are in place to prevent staff and students from accessing extremist and inappropriate materials on UCQ networks.

2.2.2 UCQ sets out to educate staff and students regarding the risks and ensure that all are aware of safe online behaviour. As a minimum, this is covered with all students during their induction.

2.2.3 All students and staff to adhere to acceptable use of IT. For staff, this is laid out in GP-013 Staff Handbook Appendix E: Communications and IT. For students, this is laid out in this policy paragraphs 6-10.

2.2.4 Staff are trained to recognise the signs of inappropriate behaviour or concerns regarding their students and report any concerns in line with SA-002 Safeguarding Policy.

2.2.5 Any reports of e-safety incidents will be acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring. Action following the report of an incident might include disciplinary action, sanctions as described in paragraph 11, reports to external agencies as appropriate, review of internal procedures and support for affected individuals.

2.3 Useful websites include:

UK Safer Internet Centre	www.saferinternet.org.uk
Child Exploitation and Online Protection Centre	www.ceop.police.uk
CEOP’s Think You Know	www.thinkuknow.co.uk
Get Safe Online	www.getsafeonline.org
Internet Matters	www.internetmatters.org

3. County lines

3.1 County lines is a term used to describe gangs or organised criminal networks involved in exporting illegal drugs into one or more importing areas, using dedicated mobile phone lines known as 'county lines' or 'deal lines'. The 2016 NCA report *'County Lines Gang Violence, Exploitation & Drug Supply'* reports that 80% of areas surveyed saw the exploitation of children and vulnerable adults by gangs. Children as young as 11 can be recruited. Gangs typically recruit and exploit vulnerable people using:

3.1.1 coercion

3.1.2 deception

3.1.3 intimidation and threats

3.1.4 violence

3.1.5 debt bondage

3.1.6 grooming

3.2 Whilst most initial contact is carried out on the street and in schools, groups have been known to use social media to entice vulnerable people in. Students should consult with UCQ staff if they have been contacted by a person not known to them or if they feel they have been targeted by one of these groups.

4. Prevent

4.1 Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies, including further and higher education institutions, to have due regard to the need to prevent people from being drawn into terrorism.

4.2 The internet, social media, and text messaging can be useful tools to reach out to young and vulnerable people to communicate extremist messages. All students should be aware of this threat and contact the UCQ Safeguarding Team as soon as possible if they, or someone they know, are engaging or asked to engage, in extremist activity online.

5. Data protection

5.1 UCQ complies with the Data Protection Act 2018 and GDPR by ensuring the personal student data is collected and processed lawfully, is processed in a manner that ensures data is secure and kept in a form which permits identification of data subjects for no longer than is necessary. UCQ's compliance is set out in DA-001 Data and Privacy Policy.

6. Using UCQ IT facilities

6.1 When using UCQ IT facilities, students must:

6.1.1 Set their password so it is strong: a minimum of eight characters in length and consists of a mixture of alpha-numeric (letters and numbers) characters. Passwords should not be set to names or words which would be easy for someone to guess. The stronger the password, the more protected the user is from hackers and malicious software.

6.1.2 Change their password regularly, at least twice a year and more often if possible.

6.1.3 Contact the IT Manager on 0191 275 5015 immediately if a virus is detected on any UCQ computer equipment.

6.1.4 Respect, and not attempt to bypass, security in place on the computer systems. Accessing, copying, removing or otherwise altering other people's work, or attempting to alter the settings of computers is not acceptable use of the equipment.

6.2 When using UCQ IT facilities, students must not:

6.2.1 Disclose their passwords to others or use passwords intended for the use of others.

6.2.2 Store, install, or attempt to install, programmes of any type on to a UCQ device .

6.2.3 Use any utility programs or software that can monitor system activity.

6.2.4 Damage, disable or otherwise harm the operation of computers, or intentionally waste limited resources. Do not deliberately attempt unauthorised access to networked facilities or services. Do not introduce data-interception, password-detecting or similar software or devices to the device or network.

6.2.5 Use the network for commercial purposes, e.g. buying or selling goods.

6.2.6 Use the network to harass, harm, offend or insult others.

6.2.7 Play any computer games.

6.2.8 Use the network on site unless they are logged on using the UCQ Student Wifi system.

6.2.9 Connect any hardware devices to the UCQ network without staff approval.

6.2.10 Create or transmit of any offensive, obscene or indecent images

6.2.11 Create or transmit any material which is subsequently used to facilitate harassment, bullying and/or victimisation or promote discrimination of any kind.

7. Internet usage

7.1 Students must:

7.1.1 Access the internet only for study purposes or for UCQ authorised activities.

7.1.2 Respect the work and ownership rights of people outside UCQ, as well as students and staff. This includes abiding by copyright laws.

7.2 Students must not:

7.2.1 Use the internet to obtain, download, send, print, and display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive. Do not access or use materials that would bring UCQ into disrepute.

7.2.2 Use the internet to access material that is extremist, or which has the potential to radicalise themselves or others.

7.2.3 Engage in online chat activities .

7.2.4 Use the internet in class without their Tutor's prior permission.

7.2.5 Download Audio or Video files without their Tutor's permission.

8. E-mail usage

8.1 Students must:

8.1.1 Report to their Tutor any unpleasant material or messages. Such reports will be treated confidentially and will help protect students.

8.2 Students must not:

8.2.1 Give personal information such as address or telephone number to those who make contact through electronic mail.

8.2.2 Use any personal laptops or other devices (using the UCQ network) except in the designated areas whilst complying with the security recommendations of UCQ.

9. Social media usage

9.1 Social media is a useful tool, however students must be aware of the risks to protect themselves and their data. Students must :

9.1.1 Assume everything online is permanent and effectively public.

9.1.2 Make sure they consider who might see anything that is posted.

9.1.3 Write appropriately for their expected audience.

9.1.4 Make all staff/student online interactions meaningful and professional.

9.1.5 Take responsibility for what they post or distribute online and specifically consider safety and reputation.

9.1.6 Use the internet positively for communication, collaboration and learning.

9.1.7 Use and maintain privacy settings to protect personal information but do not rely on them solely to protect themselves.

9.2 Students must not:

9.2.1 Post anything which might damage their own or UCQ's reputation.

9.2.2 Redistribute any material which may harm others in any way.

9.2.3 Use the internet to form, or attempt to form, any relationship which would be otherwise inappropriate.

9.2.4 Create an online environment which invites others to post harmful content.

9.2.5 Post without thinking or considering the safeguarding risks.

10. Information security

10.1 Students must:

10.1.1 Get permission from the UCQ IT Manager before storing personal details on any UCQ computer.

10.1.2 Be aware that student work (other than emails) may be backed up and archived.

10.1.3 Be aware that UCQ is required to monitor and log user activity on all networked computer systems.

10.2 Students must not:

10.2.1 Corrupt or destroy other users' data.

10.2.2 Violate the privacy of other users.

11. Sanctions

11.1 The breaking of these rules will result in withdrawal of access to UCQ's information computer technology resources.

11.2 Additional action may be taken by UCQ in line with existing practice regarding inappropriate behaviour. For serious violations, the UCQ disciplinary procedures will be implemented.

11.3 UCQ reserves the right to examine or delete any files that may be held on its computer systems or to monitor any internet sites visited.

11.4 Students must report to their tutor any security breaches. Such reports will be treated confidentially.

11.5 The UCQ IT Manager will lock student user accounts immediately after instructed to do so by a member of staff or if a virus is reported by the virus checking software. The student's Tutor will be contacted and the account will remain locked until the Tutor, having spoken to the student, instructs the IT Manager in writing to re-instate the account.

12. Monitoring

12.1 UCQ has software and systems in place to record all internet usage.

12.2 UCQ reserves the right to monitor/record usage at any time. No UCQ authorised user of the internet should have any expectation of privacy as to his or her internet usage.

12.3 The UCQ IT Manager will regularly monitor this policy in consultation with the Senior Leadership Team.

13. Initial equalities impact assessment

Department: All	**Completed by:** Tara Henderson, Head of Policy & Governance	**Date of initial assessment:** 19/01/2021
Area to be assessed:	SA-014 Safe Use of IT Policy	
Existing or new policy/procedure:	Existing	
What evidence has been used to inform the assessment and policy? (please list only)		
External guidance and requirements: ➢ Office for Students Conditions of Registration - Prevent in HE ➢ Counter-Terrorism and Security Act 2015 ➢ Data Protection Act 2018 and GDPR ➢ 2016 NCA Report 'County Lines Gang Violence, Exploitation and Drug Supply' **Internal guidance and requirements:** ➢ Consultation with IT Manager and Quality Manager ➢ DA-001 Data and Privacy Policy ➢ SA-001 Safeguarding Policy		

1. Describe the aims, objectives or purpose of the policy/procedure	UCQ fully recognise their responsibilities to safeguard all students and is committed to providing a safe environment for study and work, including a safe online environment. UCQ will do all it can to make students and staff stay safe online and to satisfy its wider duty of care. This policy encompasses both online safety and acceptable use of IT.		
2. Which stakeholders/groups are intended to benefit from this policy/procedure?	Primarily students, however staff can also benefit from this policy.		
The Equality Act 2010 requires public bodies to have 'due regard' to the need to:- (1) Eliminate unlawful discrimination, harassment and victimization (2) Advance equality of opportunity between different groups; and (3) Foster good relations between different groups	**3. Could the policy/procedure have a disproportionately negative effect impact in terms of the aims set out in (1) to (3) of the Act on any of the protected characteristics?:-** **High** **Medium** **Low** **No effect**	**4. Briefly explain how the policy/procedure furthers or prevents the aims set out in (1) to (3).**	**5. If there is a disproportionately negative impact on any protected characteristics, can it be justified on the grounds of promoting equality or any other reason? If yes, please explain.**
Protected characteristics **Age**	No effect	Not applicable	Not applicable
Disability	No effect	Not applicable	Not applicable
Gender	No effect	Not applicable	Not applicable
Gender reassignment	No effect	Not applicable	Not applicable
Marriage and Civil Partnership	No effect	Not applicable	Not applicable
Pregnancy and Maternity	No effect	Not applicable	Not applicable

	Race	No effect	Not applicable	Not applicable
	Religion or Belief	No effect	Not applicable	Not applicable
	Sexual Orientation	No effect	Not applicable	Not applicable

6. Has there been any consultation/engagement with the appropriate protected characteristics?		Not applicable as no PC impact identified
7. What action(s) will you take to reduce any disproportionately negative impact, if any?		None required
8. Based on the information in sections 1 to 7, should this policy/procedure proceed to Full Impact Assessment? (recommended if one or more 'High' under section 2)		No
Assessor signature: 	**Approved by:** **Michelle Elliott** 	**Date approved:** 19/01/2021