UCQ
UNIVERSITY
CENTRE QUAYSIDE

Safe Use of IT Policy

Version: 1
Revision date: 28/02/2020

Due for review: 28/02/2022

Table of Contents

1. Introduction

1.1 Where required, laptops are provided and maintained for the benefit of all students.

1.2 Students are encouraged to use and enjoy these resources and to ensure that they remain available to all.

1.3 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. Using UCQ IT facilities

2.1 Students must:

2.1.1 Set their password so it is a minimum of eight characters in length and consists of a mixture of alpha-numeric (letters and numbers) characters.

2.1.2 Passwords should not be set to names or words which would be easy for someone to guess.

2.1.3 Change their password at least twice a year and more often if possible.

2.1.4 Contact the IT Manager on 0191 275 5015 as soon as a virus is detected on any UCQ computer equipment.

2.1.5 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.

2.2 Students must not:

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

2.2.2 Store, install, or attempt to install, programmes of any type on to a computer.

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

2.2.4 Damage, disable or otherwise harm the operation of computers, or intentionally waste limited resources.

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

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

2.2.7 Play any computer games.

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

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

3. Internet usage

3.1 Students must:

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

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

3.2 Students must not:

3.2.1 Use the internet to obtain, download, send, print, and display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.

3.2.2 Engage in chat activities over the internet. This takes up valuable resources which could be used by other people to benefit their studies.

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

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

4. E-mail usage

4.1 Students must:

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

4.2 Students must not:

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

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

5. Social media usage

5.1 Students must:

5.1.1 Assume everything online is permanent and effectively public.

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

5.1.3 Write appropriately for their expected audience.

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

5.1.5 Consider specifically safety and reputation before posting online.

5.1.6 Take responsibility for what they post or distribute online.

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

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

5.2 Students must not:

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

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

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

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

5.2.5 Post without thinking.

5.2.6 Post without considering the safeguarding risks.

6. Information security

6.1 Students must:

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

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

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

7. County Lines

7.1 The 2016 NCA report *'County Lines Gang Violence, Exploitation & Drug Supply'* reports that 80% of areas surveyed saw the exploitation of children by gangs. Children as young as 11 can be recruited. Gangs typically recruit and exploit vulnerable people using:

7.1.1 coercion

7.1.2 deception

7.1.3 intimidation and threats

7.1.4 violence

7.1.5 debt bondage

7.1.6 grooming

7.2 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.

8. Prevent

8.1 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.

8.2 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.

9. Sanctions

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

9.2 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.

9.3 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.

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

9.5 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.

10. Monitoring

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

10.2 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.

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