The University's IT Code of Conduct

In order to use the University's IT systems and services, all 'users' (students, staff and visitors) are required to comply with the following code of conduct:

a) This policy applies to the use of any University IT facility, *including* for example the use of a personally owned device that is attached to the University's wifi or to any other University IT asset or service.

b) All users are required to report any misuse of IT systems, any infringement of this policy and any issue that may endanger full compliance with relevant UK Data Protection legislation,.

c) All *private*[1] and *confidential*[1] information (electronic and paper), and the means of accessing it (using a PC/Laptop/ Smartphone) should be physically secured (locked away) when not being used.

d) You must inform the University if you believe there may be any risk of breach or potential breach of UK Data Protection legislation through information loss, or of any unauthorised access to information.

e) You must report the loss of any computing equipment that might contain Confidential[1] information.

f) Users should not intentionally cause damage, access or alter admin device or systems settings, or otherwise jeopardise the integrity of computer equipment, software or network services.

g) Anti-virus software must be used on any personal equipment used to access University services.

h) Users must abide by all agreements and contracts by which software and any associated information are accessed using University computing services. Specifically, users must not install, replace or update information on University computing equipment without appropriate authority[2].

i) Users must not alter or install unauthorised software onto University computing equipment without appropriate authority[2].

j) Users must not take University IT equipment off-campus, without the appropriate authority[2] to do so.

k) Users must not use any University computing services to gain unauthorised access to any other computing system (internal or external). This includes any unauthorised access to any other person or organisation's computer systems or data, or any other copyrighted material[3].

l) You must not acquire or distribute *unauthorised*[1] information, and you must not use University IT systems or services for acquiring, storing, receiving or transmitting offensive, indecent or obscene material. This includes through web browsing, where using proxy-avoidance and anonymiser websites is expressly prohibited[4].

m) Information should be stored in the most suitable facility, for example if a case management system exists, related confidential information should not be stored in ad-hoc general storage such as network drives, cloud or removable media such USB Sticks.

n) Users must avoid sharing any documents or folders made available to them, particularly if these contain any private[1] or confidential[1] information.

o) Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening[5], discriminatory or extremist. The University observes the Prevent Duty of Care and reserves the right to block or monitor access to such material

p) Users must not use University IT systems or services for any commercial activity[6] without appropriate authority[2] from IT Services or their Head of Department.

q) Users are not permitted to use University IT systems and services for private commercial purposes or any other employment outside the scope of that person's official duties or functions.

r) IT Disposal – users must return any University owned IT equipment to IT Services for secure disposal.

The Code of Conduct is an integral element of the Electronic Information Security Policy, and the University's Acceptable IT use policy – please http://help.chi.ac.uk/it-strategy-and-policies

[1] For definitions of Private, Confidential and Unauthorised information please see the Electronic Information Security Policy
[2] *Appropriate authority* means, formal agreement from a relevant Head of Department and IT, recorded through the SIZ support desk.
[3] This particularly includes downloading copies of films and music outside of their copyright requirements.
[4] Exceptions can be made for the collection and storage of sensitive materials for authorised research
[5] This includes anything that might be considered as bullying, harassment or stalking
[6] This is because University equipment uses discounted HE software licensing, and when used for commercial activity, this has to be altered. to pay the full commercial license cost of the software to its supplier.