The University’s IT Code of Conduct

This policy applies to the use of any University IT facility, including any personally owned device that is attached to the University’s WiFi or to any other University IT asset or service. 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:

1. 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.
2. You must not use your University identification or passwords with non University services.
3. 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.
4. All *private*[[1]](#footnote-2) 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.
5. You must report the loss of any computing equipment that might contain confidential1 information.
6. 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.
7. Anti-virus software must be used on any personal equipment used to access University services.
8. 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]](#footnote-3).
9. Users must not alter or install software onto University computing equipment2.
10. Users must not take University IT equipment off-campus, without the appropriate authority2 to do so.
11. Users must not use any University computing services to gain unauthorised access to any computing system (internal or external). This includes unauthorised access to copyrighted, personal or confidential material[[3]](#footnote-4).
12. You must not solicit, encourage or endorse use of, any non University computer system, or use a University system in a new context without first having an (approved) Data Protection Impact Assessment.
13. 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]](#footnote-5).
14. Information should be stored in the most suitable facility, for example in a case management system or Network folder, and not in ad-hoc general storage such as cloud or removable media such USB Sticks.
15. Users must avoid sharing any documents or folders made available to them, particularly if these contain any private1 or confidential1 information.
16. Users should not transform any confidential information communicated with them (for example using a recording of a video conference or copying any email or instant messaging) to any other media or facility.
17. Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening[[5]](#footnote-6), discriminatory or extremist. The University observes the [Prevent Duty of Care](https://www.gov.uk/government/publications/prevent-duty-guidance) and reserves the right to block or monitor access to such material
18. Users must not use University IT systems or services for any commercial activity[[6]](#footnote-7) without appropriate authority2 from IT Services or their Head of Department.
19. 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.
20. 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 – which can be found at the following link: [Link to Policy](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 [↑](#footnote-ref-2)
2. If there is a specialised need, this may reviewed through IT, recorded through the SIZ support desk. [↑](#footnote-ref-3)
3. This particularly includes downloading copies of films and music outside of their copyright requirements. [↑](#footnote-ref-4)
4. Exceptions can be made for the collection and storage of sensitive materials for authorised research [↑](#footnote-ref-5)
5. This includes anything that might be considered as bullying, grooming, radicalisation, harassment or stalking [↑](#footnote-ref-6)
6. This is because University equipment uses discounted HE software licensing, and commercial licenses may be required. [↑](#footnote-ref-7)