

# PSE3. IT Regulations and Code of Conduct

## 1. Access to IT Resources

Members of the CITY ULE, including all students, are provided with a username and password to allow them free remote access to University resources required for the completion of their studies. Students must also register to the University of York Computing Services in order to activate their accounts and comply with the University of York [Using University Information Regulations](#).

Students are provided with a username and password to allow them free of charge access to the CITY ULE Computing facilities and services required for the completion of their studies. Students must sign a declaration undertaking to observe the Regulations of the CITY ULE Computing Facilities.

Students from the University of York shall be entitled to access the CITY ULE Computing Facilities during their visit to the CITY ULE.

## 2. Code of Practice for the Use of Computing Facilities

Computing facilities are owned by the CITY ULE and situated on all premises.

No food or drinks are allowed to be consumed in the Computing Facilities.

The facilities are strictly no smoking areas.

Users shall not:

- interfere with other people's use of the network or offend them, or invade their privacy;
- use another person's password to gain unauthorised access, or allow their own password to be used to give another person unauthorised access;
- use any software or equipment for any profit making activity. Copying software or using unauthorised copied software is strictly forbidden;
- delete, modify or install any software on PCs or remove the cover of a PC;
- reserve a PC for more than 15 minutes while they are away from labs.

Internet access should be used only for academic reasons. Games, chat and downloading of irrelevant material are not allowed. Also, access to illegal sites or sites with mature content is strictly forbidden.

The IT System Administrator monitors activity on all machines (including internet access). All Internet sites visited by users are monitored. Information that is registered includes: username, PC, Time accessed, Type of information accessed.

The IT System Administrator must not abuse his power by eavesdropping but they are permitted to observe users if abuse of the network is suspected.

Users are allowed to connect a wireless device to the network but must have some form of up-to-date anti-virus protection on the device.

The CITY ULE Computing Facilities are under 24 hours surveillance (recorded) for the security of the establishment.

If users are found to be in breach of any of the code of practice for Computing Facilities, then the CITY ULE may exclude the users from access to its computing facilities for an indefinite period. In more serious cases, regulations relating to discipline of students will apply.