Regulation XXIV:
Regulations on the Use of IT Facilities

1. In these Regulations **"Information Technology (IT) Facilities"** means any computing services, devices or systems:

   (a) controlled or operating on behalf of the University;
   (b) owned by the University or any University company;
   (c) situated on University premises or connecting to University IT systems.

   This includes hardware, software, physical spaces (e.g. open access computer rooms, data centres) and third-party services (e.g. online cloud services) provided by the University for the purposes of processing information.

   "Head of Department/School" means the Head or Chair of the Department/School which controls the facilities or the premises on which the facilities are situated.

2. No person may use IT Facilities without the authorisation of the Chief Information Security Officer (CISO), Director or Assistant Directors of IT Services, acting on behalf of the University, or of the Head of Department/School or of the person or body to whom the facilities belong.

3. Every authorisation for the use of IT Facilities will be subject to the conditions that the facilities are to be used only by the person(s) to whom the authorisation is given and only for the purpose or purposes for which it was granted and will be subject to these Regulations, relevant legislation and University policies and procedures.

4. The IT facilities are provided for use in furthering the mission of the University of Sheffield. University IT accounts shall not be used for personal activities.

5. Where the use of IT Facilities is for the purposes of externally funded research or for purposes private to an individual user or external to the university, authorisation may be subject to the payment of charges prescribed from time to time by the UEB IT Sub-Group or by the Chief Information Security Officer (CISO), Director or Assistant Directors of IT Services, acting in accordance with any directions of that Sub-Group.

6. No IT Facilities may be used:

   (a) to secure unauthorised access to any program or data held in any computer, wherever located;
   (b) to cause any unauthorised modification of the contents of any computer, wherever located;
   (c) in any way which jeopardises the work of others, or the integrity of the equipment or of any programs or data;
   (d) in breach of the Computer Misuse Act 1990 or other applicable legislation, or of any local rules made by the Chief Information Security Officer (CISO), Director or Assistant Directors of IT Services or the Head of Department/School.

7. No student or member of the University staff may use any means:

   (a) to secure unauthorised access to any program or data held in any IT Facilities;
   (b) to cause any unauthorised modification of any such material.

8. Any breach of these Regulations may be dealt with, in the case of students under the Discipline Regulations and in the case of members of the staff of the University in accordance with disciplinary procedures approved (subject to the Statutes) by the Council. Any person

suspected of a breach of these Regulations may be debarred from access to IT Facilities by the Chief Information Security Officer (CISO), Director or Assistant Directors of IT Services or the Head of Department/School until the appropriate disciplinary procedures have been completed; any use or attempted use of facilities by a person so debarred from access or by another acting on that person's behalf will constitute a breach of these Regulations.

Note: These Regulations should be read in conjunction with the **IT Code of Practice** – https://www.sheffield.ac.uk/it-services/codeofpractice.