STRANMILLIS UNIVERSITY COLLEGE

A College of Queen's University Belfast

IT Systems
Regulations for Acceptable Use

OBJECTIVE

To maximize the benefits of the University College computer resources and minimize potential liability.

Notes

> The purpose of these regulations is to make users aware of their duty to use the University College's computer resources responsibly, professionally, ethically and lawfully.

> It is the responsibility of **each** user to adhere to these regulations. Users in **breach** of these regulations **will be liable to disciplinary action** under University College procedures.

1   e.g. Legislation relating to:-
   i.   Interception of Telecommunications
   ii. Telecommunications for Lawful Business Practice
   iii. Human Rights
   iv. Data Protection
   v. Computer Misuse
   vi. Terrorism
   vii. Copyright

> Comply with all **applicable laws.**[1]

> Do not send or request **inappropriate or unlawful material**[2] or deliberately download, store, or view such material.

2   Material that is fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate.

> Comply with the **JANET Acceptable use Policy,**[3] http://www.ja.net/documents/use.html

> Do not allow third parties to use your account. Account holders are responsible for all computer activity performed using their account.

3   Avoid the following:-
   i.   creation or transmission of material likely to cause annoyance, inconvenience or needless anxiety
   ii. transmission of unsolicited commercial or advertising material

> Do not deliberately **waste resources.**[4] IT facilities are provided solely to support the academic functions of the University College.

> Identify yourself **honestly and accurately** when communicating online

4   This includes, but is not limited to, sending mass mailings, chain letters, subscribing to non business related email lists, engaging in unauthorised chat forums.

> Do not engage in conduct likely to jeopardise or interfere with the integrity of the computing equipment, its programs or other stored information.

5   Occasional and reasonable personal use is permitted provided it does not interfere with performance of duties.

> Respect the copyright of all materials and not use, download, copy, store or supply copyright materials including software and retrieved data other than with the permission of the copyright holder or under the terms of the licence held by the University College.

6   Staff must be aware that access to their email may be gained for business operational/continuity needs.

> Users must not connect equipment to the University College network without authorisation from IT Services.

> Email is primarily for **University College use.**[5&6]

> "Broadcast" email distribution lists should be used sparingly and only for College purposes[7]. Users wishing to send out information which is not associated with the business of the College, but which they feel may be appropriate should request clearance from the Principal's office first.

7   Staff and student distributions lists should not be used to promote personal viewpoints of a political, religious or any other nature.

➢ **Breaches of these rules**, actual or suspected, should be reported to **IT Services ext 242, email ITManager@stran.ac.uk**.

➢ Incoming and outgoing emails will be scanned by automated systems to remove potentially harmful attachments. Access to the World Wide Web will also be filtered by an automated system to block potentially inappropriate sites. Attempts to access blocked sites are logged.

➢ In keeping with the Regulation of Investigatory Powers Act, the University College reserves the right to monitor[8] remotely and record computer use. If this monitoring should indicate that an abuse of IT facilities is likely to be taking place then further appropriate investigation of user activity may following including, for example, the examination of emails, internet use and document storage.

➢ These regulations should be read in conjunction with the Information Security Policy Statement and the Data Protection Regulations.