Rules of Use

I. Eligible Users

College ICT Resources are provided only for use by staff, students and authorized visitors of St. Mary’s University College.

- College facilities may not be used by members of the general public;
- nor by former students of the College;
- nor by family members of staff or students of the College;
- nor by former staff of the College;
- nor by members of any other institution without prior authorisation.

Exceptions may be permitted with the agreement of the Computing Services Manager.

II. C&IT users must:

1. Sign the Computer Users Agreement before accessing any of the College IT facilities.

2. observe all applicable laws and regulations relating to the use of ICT equipment, notably:
   - comply with the Computer Misuse Act 1990 which makes activities such as hacking or the deliberate introduction of viruses a criminal offence;
     (Hacking is defined as unauthorised access to a computer system (locally or through a network) for the purpose of obtaining another’s identifier and password, or using resources that have not been allocated, with intent to modify or damage another’s files or systems files, or to obtain or alter financial or administrative records, or to facilitate the commission of a serious crime).
   - comply with the Criminal Justice Act 1994 amendment to the Obscene Publications Act under which it is a criminal offence to create, store, download or transmit obscene material. This includes the storage of files sent to users as e-mail attachments.
   - respect the copyright of all materials and software that are made available by College service providers and third parties for authorised use;
     Users must abide by the CHEST Code Of Conduct For The Use Of Software Or Datasets (see http://www.eduserv.org.uk/licence-negotiation/agreements/User%20Obligations) and Copyright Law (Copyright Act 1956 and Copyright, Designs and Patents Act 1988). In particular users must not make, run or use unlicensed copies of software or data;
   - familiarise themselves with and comply with the requirements of GDPR and the Data Protection Act (see https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/introduction-to-data-protection/);
     The College is registered with the UK Data Protection authorities. Data Protection laws protect individuals against the unauthorised use or disclosure of their data. The misuse or disclosure of an individual’s data outside of the administrative processes of the College may amount to a criminal offence. The College may regard non-observance of Data Protection Laws as a disciplinary offence.

3. agree to pay such charges as may be incurred for the use of facilities or services (principally laser/colour printing).

4. only use the facilities for their academic work, except for limited, non-remunerative personal use. Personal use of College systems that incurs any form of cost to the College (including resource consumption such as electricity) or has any impact on staff or students (including on their time) is not permitted. As examples, the use of College PCs for bitcoin mining is excluded by the first condition, and the non-academic use of email distribution lists is excluded by the second. Users must report to the College, immediately it comes to their notice, any reasonable probability of financial or commercial advantage arising out of their use of the
resources, whenever this advantage would accrue and whoever would benefit. They agree to abide by the
general conditions in force in the College on the exploitation of such financial or commercial benefits.

5. treat as confidential, and as private property, all information and software which may accidentally become
available to them. They agree not to copy, retain, modify or disseminate any part of such material.

6. understand that evasion or attempted evasion of security mechanisms, and deliberate eavesdropping are
forbidden and liable to disciplinary procedures.

7. understand that the College may at any time monitor any use of the resources either for reasons of system
maintenance or to ensure that College Regulations and the law of the land are not being violated. Such
monitoring will be in compliance with the Regulation of Investigatory Powers Act 2000

III. C&IT users must not:

1. use material or programs in such a way as to contravene the law;

2. use the facilities in such a way as to risk or to cause loss, damage or destruction of data or breaches of
confidentiality of data;

   Computing Services undertakes to provide appropriate security measures to limit the likelihood of such
occurrences on centrally managed systems. However Computing Services cannot give any warranty or
undertaking about the integrity of information stored on College systems.

3. jeopardise the provision of services (for example by using resources for recreational purposes or by
inappropriate use of bulk email), or use the resources in such a way that the work of other users, the integrity
of the computing equipment or any stored programs or data may be jeopardised;

4. engage in software theft or abuse of software licence (see http://www.fast.org.uk);

5. use the facilities in such a way that brings or could bring the College into disrepute;

   Users will be held personally liable and may be subject to disciplinary proceedings, for example for issuing
false or libellous statements or for breaching the copyright of others.

6. allow their account to be used by others, or disclose passwords to others, or use accounts or passwords
belonging to others;

7. do or fail to do anything which has the result of introducing any virus, worm, malware, spyware, adware or
other harmful program to any computer, file or software on the system (this obligation includes doing anything
to circumvent any firewall or software designed to protect systems against harm);

8. interfere or attempt to interfere with or destroy systems or software set up on shared facilities (this obligation
includes loading or attempting to load unauthorised software on podium PCs);

9. attempt to open, move, disconnect or in any other way tamper with or attempt to destroy or damage any I.C.T.
equipment; or interfere with, disconnect, damage or remove without authority any equipment made available for
use in conjunction with any College ICT facilities;

10. attempt to rectify faults in equipment. All faults should be reported to Computing Services;

11. smoke, eat, drink or use mobile phones in rooms containing computer equipment;

12. use College equipment to carry out unauthorised actions at other institutions or organisations;

13. leave a workstation or PC which they have logged into unattended for any length of time; (users who do so risk
having someone access their account, possibly abusing their identity, for which they may then be liable).
Student workstations automatically log-off the logged-in user after fifteen minutes of inactivity, but this
presents a window of opportunity for mischief if a user leaves a machine logged-in and unattended;

14. run any software to prevent others from using the PC or workstation when they leave the station;
15. remove, deface or destroy output not originated by them;
16. attempt to connect any items of equipment to a PC, printer or network connection belonging to the College without obtaining prior permission from Computing Services;
17. use College resources to write or develop software or any other electronic resource (e.g. websites) except in direct connection with their academic coursework, and this must not contravene II.4 above.
18. use their College password, or any obvious variant of it, as their password for any online service.

IV. Conditions of Use

Use of the College ICT facilities is subject to the following conditions of use:

1. The facilities (including software) are provided entirely at the risk of the user. The College will not be liable for loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), damage (including damage to hardware, software or data) or inconvenience arising directly or indirectly from the use of the facilities, except where statutory health or safety matters are involved.

2. The College reserves the right to inspect, copy, modify and/or retain user data in order to investigate operational problems or for the investigation of suspected misuse. The College also reserves the right to take whatever remedial action it considers necessary should misuse occur. (For example, if an email is circulated that is likely to cause upset or offence, the college may choose to automatically move this email from each user’s Inbox to their Junk mail). Any such action by the college will be in compliance with the relevant legislation.

3. The College accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or the invalidation of any warranty agreement) to equipment not owned by the College as a consequence of any work carried out on such equipment by members of staff, whether authorised or not.

4. The College accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or invalidation of any warranty agreement) to equipment not owned by the College as a consequence of direct or indirect connection, whether authorised or not, to the College networks. The user shall indemnify the College for any loss or damage, whether direct or indirect, suffered or incurred as a consequence of the interconnection of any hardware or software not owned by or under the control of the College with any IT system, hardware, software or data owned or controlled by the College.

5. Use of College systems is on the understanding that once a user ceases to be a member of the College community, they will no longer have access to the ICT facilities. Prior to cessation of access, there should be no need to transfer off College systems any personal files, email correspondence and any other material that a user wishes to retain since such material should not be stored on college systems.

V. Responsible Use

In using the computing facilities provided by the College, you are expected to act responsibly.

Failing to act responsibly – knowingly or unknowingly – may result in your user account being disabled, without prior warning, by College Computing Services. You may also be subject to further College disciplinary procedures. By observing the practices laid out in this document, you should be able to avoid these measures.

Rules Of Use Change Log