# ICT Acceptable Use Policy

These are the rules and guidelines to be followed by all students and staff when using IT facilities at Holy Cross College. Further information regarding the IT facilities at Holy Cross College is available in the student packs given out during induction, or via the IT Help Desk in IT 4 (on the 1st floor of the Mary Kelly Building).

In addition to the rules presented in this document all users of the college systems must also comply with all applicable laws and regulations relating to the use of Information Technology. This includes, but is not restricted to:

- Computer Misuse Act (1990) which makes activities such as hacking or the deliberate introduction of viruses a criminal offence
- 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
- Data Protection Act 1998
- Respecting the copyright of all materials and software made available by the College or third parties for authorised use
- The regulations set out by JANET, the electronic communications network and associated electronic communications networking services and facilities which supports the requirements

*Staff should also be aware that this document only includes instructions that are relevant to students and staff. Other rules relevant to staff are included in the full college* ***Information Security Management (ISM) Policies*** *available in the Staff Documents area of Moodle.*

## 1. Introduction

Holy Cross College has made a considerable investment in its IT facilities over recent years to ensure that students and staff are able to embrace the use of new technology. This includes a powerful network of computers with Internet, Intranet and e-mail facilities for everyone. Students and staff can opt to be able to access the Intranet home using their login and password (see the 'Intranet from Home' links on the Moodle Intranet site). All users must comply with the procedures, ethics and security involved in using these systems. If you need any help with the IT facilities please see a member of the IT Team at the Help Desk.

## 2. Acceptable and Unacceptable Use

The IT facilities are provided for the purpose of fulfilling the educational objectives of the college and to assist you with your studies or work at the college. It is impossible to define every specific allowed use but examples of acceptable use include research for assignments and assessments, using online learning materials, or participating in discussion groups appropriate to your course.

Users of the IT facilities at the college **must not**:

- Create or transmit any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material. Some areas of the internet contain information or media which could cause offence to other people or may be illegal to download or view. Examples of misuse include uploading images or videos which show antisocial behaviour or illegal activities; making derogatory statements about the college, college staff or other students; or revealing confidential information about the college, college staff or other students. This list is not exhaustive. You are prohibited from knowingly accessing, viewing or downloading such material.
- Create or transmit any material of a sexist or racist nature, or any other material in contravention of the Equality Act 2010, or material of a libellous or of a terrorist nature.
- Create or transmit any material in violation of any United Kingdom law or college regulation. This includes, but is not limited to, copyright material, threatening or obscene material, or material protected by the trade secret act.
- Use college systems for private business activities or product advertisement is generally not acceptable.
- Access material that involve extremist organisations and/or promote beliefs contrary to British values. As required under the UK government Prevent strategy.
- Bring the college into disrepute through use of online, 'social networking' activities.
- Transmit unsolicited, commercial or advertising material to other users.
- Use or produce materials to attempt to gain unauthorised access to the college IT facilities, or those of other organisations, including network scanning or probing activities
- Use or produce material which attempt to facilitate unauthorised changes or malfunctions to the college IT Services
- Create or transmit material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- Create or transmit defamatory material;
- Transmit material or use software which infringes the copyright of another person or third party;
- Download, copy, store or supply copyright materials including software and retrieved data without the permission of the Copyright holder or under the terms of the licence held by the College;
- Create or transmit material which is likely to bring the College into disrepute
- Engage in deliberate activities with any of the following characteristics:
    - Wasting staff effort or IT resources including time on end systems
    - Corrupting or destroying other users' data;
    - Violating the privacy of other users;
    - Disrupting the work of other users;
    - Preventing others from accessing a workstation when they are no longer using it
- Continue to use an item of networked software or hardware after the College has requested that use cease because it is causing disruption to the current functioning of the network;
- Engage in other misuses of the network or networked resources, such as the introduction of 'viruses'
- Play online games other than those created for learning purposes and authorised by the IT Department

- Use chat-sites, or social media sites unless authorised by the college.
- Engage in any other actions that infringe current legislation.
- Allow their account to be used by others or disclose their passwords to others
- Use accounts or passwords belonging to others
- Engage in software theft or abuse of software licenses
- Forge e-mail signatures or use College logos for unauthorised purposes
- Initiate and / or forward ‘chain’ or ‘junk’ e-mail
- Interfere or attempt to interfere with or destroy systems or software set up on college systems. This includes the loading or attempting to load unauthorised software onto college systems
- Attempt to open, move, disconnect or in any other way tamper with or attempt to destroy or damage Information Technology equipment. All faults with equipment should be notified to the IT Department
- Remove, deface or destroy output not originated by the user
- Attempt to connect any items of equipment belonging to the University without obtaining prior permission.

## 3. Network Accounts

All members of the college are given an account on the network that requires a username and password. It is the responsibility of each member to ensure that they:

- Change their password to a complex password that is difficult for anyone else to guess, preferably using a mix of letters and numbers and symbols.
- Ensure that the password is not one that you use on other systems or have used in past.
- Do not allow anyone else to use their account, or leave their account logged on and unattended at any time.
- Try to ensure that no one can watch them typing in their password.
- Log-off their PC (or lock the PC if you are a staff member) before leaving it for any period of time.
- Inform the IT staff if there is any evidence of someone else using, or attempting to use, their account or if they identify a security problem on the network.
- Do not attempt to gain access to any other user’s account or attempt to discover anyone’s password or carry out other activities usually referred to as ‘hacking’.

## 4. Use of IT suites

- No programs should be run or installed at Holy Cross College unless it has been installed by the IT Department or clearly approved by them.
- Computer games are NOT permitted unless permission is given by the IT Department.
- No food or drink may be consumed in any of the IT Suites or the Library at any time. This includes during timetabled lessons. Chewing gum and sweets are forbidden.
- Always try to keep the IT Suites tidy by disposing of waste paper, putting the chairs under the desk etc.
- Always log-off the PC’s when you’ve finished.

- The open access area (IT3 and IT4) is a designated quiet study area. Groups of students around PCs and loud conversation will not be tolerated. Teaching staff should take this into account and book an IT suite if group work is required as the open access areas are not suitable for this purpose.
- The open access area (IT8) is a designated silent study area. Talking, working in groups or distracting other students in the IT Suite will not be tolerated.
- The IT suites are not cloakrooms - always take your belongings with you when you leave the open access IT suites – any bags left unattended will be removed.

### 5. Personal safety when using the Internet

There is evidence that some websites, including those used for academic purposes, are accessed by users who wish to exploit young people. You are advised to exercise care when communicating through the internet with people you do not know personally. The following guidelines should be followed:

- Never arrange a meeting alone with someone you have made contact with on the internet
- Never disclose any personal information through the internet to unknown persons or organisations
- Be aware that any unknown persons you are communicating with through the internet may not be who you think they are and photographs they display may not be their own.

### 6. Saving and backing up your work

- Work should only ever be saved into a user's designated user area, shared areas, or college provided cloud storage (currently OneDrive available through Office 365). Backup copies may also be stored on USB flash drives though this should never include personal data.
- Data held in your areas should be relevant to the educational objectives of the college.
- Data saved to your network account or shared area is backed-up every day and can usually be recovered even after several weeks have passed.
- Data saved to the Office 365 Onedrive or Sharepoint storage is not backed up by the college but any deleted files are retained for 90 days in the 'recycle bin' on the Onedrive site.

### 7. Use of Portable data storage devices (memory sticks, etc.)

You are encouraged to avoid the use of portable memory devices and to use web based (cloud) storage such as your college OneDrive account instead. Portable storage devices regularly fail and can be lost and should only ever be used to backup files that you have stored elsewhere. If you insist on using portable storage devices then:

- Do not store personal data (any data which would be convered by the data protection act).
- You are responsible for the information and data held on your USB memory devices.
- You can only use your own data storage device if it does do not require a mains electricity supply

- Powered data storage devices can only be used if they are college property and are supplied through the college's IT Services.
- You are personally responsible for the correct use of your data storage device. The college will not accept responsibility for any data loss or damage to devices caused by incorrect connection, ejection or shutting down of computers.
- Data storage devices must not interfere with the set-up of any college computer hardware or software. You are therefore not permitted to use data storage devices containing computer games, viruses, public domain software (free software), shareware, illegal copies of any kind, pornography or other offensive materials
- To ensure that your storage devices are virus free you should only use these on equipment with up to date anti-virus software. If you are unsure about this, scan your device using the college's virus protection software before use.
- Sensitive data or data generated and owned by the college, members of staff or other students, must not be copied or removed from the network without consent.

## 8. Accessing the wireless network using own devices (laptops, tablets, phones)

- Students and staff can connect their own devices to the college wifi network to access the Internet.
- Usage is monitored and the acceptable use policies in this document apply to the use of these devices while they are using the wi-fi network.
- Students and staff must register their devices before accessing the network using the 'Wireless Devices' page within the Student Information area on Moodle (if you are a student) or via the staff menu on Moodle (if you are a member of staff).
- Staff can request guest access for visitors who may wish to use the wireless network at the Help Desk. There is a form available which can be filled in ahead of a visit to save time. Guest users of the network are also expected to follow this acceptable use policy.
- For further information visit the IT Help Moodle Site.

## 9. Data Protection

The College must follow some rules too. We need to gather, process and store some personal data from you so that we can provide an excellent service. The government says that the data we collect must be:

- processed fairly and lawfully
- obtained for a specified and lawful purpose and shall be processed only for that purpose
- adequate, relevant and not excessive for those purposes
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary for that purpose
- processed in accordance with the data subject's (your) rights
- kept secure from unauthorised or unlawful processing and protected against accidental loss
- kept within the European Economic Area, or otherwise transferred with adequate protection

These rules are set out in the Data Protection Act 1998.

## 10. Intellectual Property Rights – Copyright

Copyright laws allow owners of copyrights to take legal action where materials are used without permission. Copyright laws may apply to materials published on the internet (such as text, audio, videos, movies, music or graphics), even if there is no direct statement on a website about copyright. Users of the college network and IT facilities must follow the copyright laws. If in doubt, staff should refer to the full ISM policies for further guidance and students should ask their teachers for advice.

## 11. Health and Safety

This section of the policy gives guidance for protecting your health and safety while using college computers. It is your responsibility to:

- take regular breaks from the computer screen
- adjust chairs to support the lower back
- maintain an upright position above waist level
- tilt the keyboard using the ‘props’ at the back
- type with your wrists straight and with your hands in line with your arms
- place the mouse at a comfortable distance from the edge of the table to avoid stretching your arms
- adjust the screen so that your eyes are at the same level as the top of the screen
- position the screen appropriately to avoid glare and adjust the brightness of the screen to the lighting conditions of the room
- leave enough room under the desk for free movement of legs
- change sitting positions from time to time

## 12. Printing

- The college is committed to reducing the environmental impact of its activities, including the use of paper for printing. All students and staff are asked to support this aim. Please only print out documents when essential.
- All printers require printing credits although staff can charge their printing to their departmental accounts.
- Students are given some printing credits free each year and can purchase additional printing credits from the help desk or library.
- A number of multifunction print devices are available for staff and student use. The printers that can be used by students are located in the following areas:

| Building | Floor | Location |
|---|---|---|
| Mary Kelly | Ground | Print room outside University Centre Office |
| Mary Kelly | First | Outside IT office |
| Mary Kelly | Second | Library |
| Marie-Therese | First | In corridor near Lift |
| Maureen Haverty | Ground | In print room |
| Emilie-Mary | First | In Chemistry resource room |

- These multi-function printing devices can be used for printing, photo copying and scanning. Print jobs sent to the ‘Holy Cross Mono’ or ‘Holy Cross Colour’ printing queues can be collected at any of these printers by using the id/swipe cards provided.
- In some areas of the college, such as Art and the Media Edit Suite, there are desktop printers available which use the same printer credits.
- See the instructions near to the multi-function printers or on the IT Help pages on Moodle for further instructions and current costs.

## 13. Monitoring and Penalties for Improper Use

It is a condition of being a student at this college that you comply with this policy. If there is anything in this policy that you do not understand, please reread it and/or contact your tutor or a college manager for guidance.

Failure to comply with this policy may result in suspension of access to the network and/or disciplinary action.

The college reserves the right to review any material in a user’s account to ensure that these rules are being followed. Any files found in the user’s account in contravention of this may be deleted without notice and disciplinary action taken.

If you witness actions or behaviour by other students that is in breach of this policy, or notice any equipment that has been damaged or does not work, please bring it to the attention of your tutor, a manager or a member of college staff.

All data and programs that have been created, owned, and/or stored by the user on or connected to the College IT facilities may, in the instance of suspected wrong doing, be subjected to inspection by the College or by statutory bodies. In the event that the data or programs are encrypted or password protected, the user will be required to provide the decryption key or password.

As provided by the Telecommunications (Lawful Business Practice) (Interception of communications) Regulations 2000, the College will intercept and monitor electronic communications for the purposes permitted under these Regulations.

In line with the requirements of the JANET Acceptable Use policy, the College will keep logs of user access and their location in order to notify the user of a reported breach of the JANET regulations.