D03 INFORMATION SECURITY POLICY

Student Use of IT

Policy Reference Number	**D038.1**
Version	2
Originator	Martin Sullivan
Approved	Finance & General Purposes Committee: 17 June 2014 Minor amendments at CLT: December 2016
Issue Date	January 2017
Review Date	Annually

A Introduction

A.1 The College is committed to providing high quality IT resources to enhance the teaching and learning that students receive.

A.2 Digital technologies have become integral to the lives of young adults both whether inside or outside the College. These technologies are powerful tools, which open up new opportunities for everyone who can access them; they can be used to stimulate debate, conduct research, produce homework, coursework and assignments and can be used to access online resources and they can be used to enhance creativity and can stimulate awareness of context to promote effective learning.

A.3 All users of the network including students have the entitlement to safe internet access and understand that the College facilities have content filtering and that it is against College policy for users to try and subvert the filtering systems in place.

A.4 All users of the network including students will be monitored and the monitoring can be used for training and disciplinary purposes. All data on the College system belongs to the College.

A.5 All users of the network, including staff are expected to adhere to JANET Acceptable Use Policy (available at https://community.jisc.ac.uk/library/acceptable-use-policy) and when using the wireless network.

A.6 All users of the EduRoam network should adhere to any additional guidelines present in the place from which you are accessing the internet.

B Personal Safety

B.1 Students may use the College's IT facilities and must do so in a responsible way ensuring that there is no risk to their own safety or the safety and security of other users of the College's facilities. These are detailed in the student acceptable use policy.

B.2 Students will only use devices that connect to the College wireless system and are not allowed to connect devices to the Colleges wired network.

B.3 Students are allowed to connect storage devices to the USB ports on the College's computers for the sole purpose of transferring their own work and research between their home computer and their home network. Students are encouraged to use more reliable forms of transferring data, including the use of cloud storage via Microsoft or google.

B.4 Students using College photographic and video facilities must ensure they have the permission of all students and staff featured in the material.

B.5 Unacceptable use of College IT facilities is regarded as misconduct. If students are discovered or suspected of doing anything against the College's Acceptable Use Policy, the College will investigate and, if appropriate, take action using the College's disciplinary procedures. This will be set out in the College Acceptable Use Guidelines that students must adhere to if they are using any of the College facilities including through remote access and via mobile devices.

D03 INFORMATION SECURITY POLICY

Student Acceptable Use Guidelines

Policy Reference Number	**D038.2**
Version	2
Originator	Martin Sullivan
Approved	Finance & General Purposes Committee: 17 June 2014 Minor amendments at CLT: December 2016
Issue Date	January 2017
Review Date	Annually

A Introduction

A.1 These guidelines form part of the Information Security Policy and set out the responsibilities and required behaviour of all users of the College's information systems, networks and computers. The full set of these policies are available from the College.

A.2 All users of the network including students have the entitlement to safe internet access. Students must understand that the College facilities have content filtering and that it is against College policy to try and subvert the filtering systems in place. Please also be aware that student activity on the College facilities may be monitored for any reason including monitoring of safeguarding, bullying, e-safety and Prevent compliance as well as monitoring of compliance with various other College policies, and that all data on the College system belongs to the College.

A.3 All users of the network including students are expected to adhere to JISC/JANET guidelines and when using the wireless network should all also adhere to the EduRoam guidelines. These specific guidelines also apply if the College facilities are accessed through any remote connection, or use of any Cloud based system provided to students by the College.

A.4 These acceptable use guidelines are intended to ensure that:

- all students will be responsible users and stay safe while using the internet and other digital technologies for educational and personal use;
- the College facilities and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

A.5 The College endeavours to ensure that students have good access to digital technologies to enhance learning and will, in return, expect each student to agree to be a responsible user.

A.6 Access to the other C=college and university networks may be granted to students if the institution is registered with EduRoam. In using other institutions' networks, students must be compliant with the EduRoam policies and procedures, our 'Student Acceptable Use Guidelines' and the all policies and procedures of the network that are being used. By using the College facilities, students must accept that they will abide by all these guidelines.

B Acceptable Use Guidelines

B.1 Students must use the College's IT systems in a responsible way, to ensure that there is no risk to the students' safety or to the safety and security of others.

B.2 For students' own safety:

- they must understand that the College will monitor my use of all its systems, devices and communications;
- they will be issued with a unique identifier (userID). This userID should not be used by anyone other than the student it is issued to, and the student should not use any other person's userID. Students must not disclose passwords to anyone else and are expected to remember passwords and not to write them down. Students will also be required to change passwords if there is any suspicion that they may have been compromised, or when asked to do so by the Vice-Principal or IT Services;
- they should be aware of the dangers of communicating with strangers when online, and should not disclose or share personal information with others. This includes, but is not limited to, name, address, telephone numbers, email addresses, age, gender, educational details, financial details etc;
- if a student chooses to meet someone he/she met online, then he/she will meet in a public place and take someone with him/her and make sure an adult knows where he/she has gone and why;
- they will report any unpleasant or inappropriate material or messages or anything that they feel uncomfortable with when they see it online.

B.3 To ensure everyone including yourself has equal rights to use technology, a student will:

- use the College systems primarily for educational purposes and only use the wireless network for personal or recreational use when not in a class.
- release College equipment that the student is using, for students that require it to complete College work;
- not make large downloads or uploads unless the student has permission form a member of staff;
- only use the internet for research and other activities that are compliant with British values unless permission has been specifically gained from a member of staff and then this is only for the purposes of debating controversial issues in a supervised activity.

B.4 Students should act as they would expect others to act towards themselves:

- respect others' work and property and will not access, copy, remove or alter anyone else's files without the express permission of the other person;
- be polite and responsible when communicating with others; not use strong, aggressive, rude or other inappropriate language and recognise the right for other people to hold different opinions;
- not take or distribute images or other information about anyone else without their permission.

B.5 Students must recognise that the College has a responsibility to maintain the security and integrity of its facilities:

- students' equipment may only be connected to the College's wireless network and must not be connected to any network socket;
- USB storage devices may be connected to College equipment but otherwise, only College owned peripheral devices may be connected to College equipment unless explicit permission is obtained from IT Services;.
- students must use IT equipment in accordance with all the rules laid out in this agreement and will comply in aiding the College in any investigation by allowing a senior member of staff to review personal devices;

- students must not access, download, distribute or otherwise use any material which is illegal, inappropriate, immoral or likely to cause others offence;
- students must not download or install any software onto any device owned by the College;
- students will not use any software on personal devices that can be used to circumvent filtering or security systems including the use of proxy addresses or VPN connections;
- any damage or faults involving College systems or software must be reported immediately, however this may have happened;
- hyperlinks in emails or email attachments must not be opened unless the person or organisation who sent the email is known and trusted, or if there are any concerns about the validity of that email. Students need to recognise the dangers - that attachments and links can contain viruses and malware that could destroy the student's and other's work;
- computers and other equipment used to access College facilities must not be left unattended and unlocked if logged in. Students must ensure that computers or other equipment is locked before being left unattended, eg by pressing ⊞ + L

B.6 Students recognise that the Internet is a useful tool for research and recreation, but must understand that:

- they should ensure they have the requisite permissions to use any original work in personal work, that this work is referenced, and agree that any work submitted to the College can be checked using plagiarism software;
- they should check to see if any work is protected by copyright and will not download illegal copies of any files eg music, videos, books etc;
- they should check to see if the information is accurate and realise that the work may be biased and misleading and will treat it accordingly.

B.7 Students must understand that they are responsible for their actions both in and out of College. In addition, students must understand that:

- the College has the right to take appropriate action against a student if he/she is involved in incidents of inappropriate behaviour whether inside the College or not;
- that if students fail to comply with this agreement and associated policies they will be subject to disciplinary action by a member of staff at the College . The outcome of any investigation to any serious breach of these guideline and its associated policies will be carried out by a senior member of staff and any illegal activity will be reported to the police or other legal authority.

C. Summary

C.1 By being a member of the College, students accept and agree to follow these guidelines when:

- using any of the College's facilities;
- using personal devices connected to any of the College's facilities, eg wireless network, USB port, charging point etc;
- using personal equipment outside of College in any way that is related to being a member of this College, eg communicating with other members of the College (whether or not they were friends prior to coming to the College), using College email, Moodle, Tyber, website or any other facility.