Student IT Acceptable Use Policy

Policy Title:	Student IT Acceptable Use Policy
Issue date (m/y):	March 2017 (update August 2019)
Author(s):	Director of IT Services and Director of Quality, Teacher Development, Student Progress and Foundation Learning
Approved by:	SMT
Date of Equality Assessment:	August 2019
Review date:	June 2021
Related Policies & Procedures:	Safeguarding Children & Vulnerable Adults Policy Supporting Student Achievement Policy E-Safety Policy Student Anti-Bullying / Harassment Policy Preventing Extremism & Radicalisation Safeguarding Policy

Equality Impact Assessment Tool

Name of Policy: Student IT Acceptable Use Policy

		Yes/No	Comments
1	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	Race or ethnicity	No	
	Disability	No	
	Gender	No	
	Religion or belief	No	
	Sexual orientation	No	
	Age	No	
	Marriage and Civil Partnership	No	
	Maternity and Pregnancy	No	
	Gender Reassignment	No	
2	**Is there any evidence that some groups are affected differently?**	No	
3	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4	**Is the impact of the policy/guidance likely to be negative/**	No	
5	**If so, can the impact be avoided?**	N/A	
6	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7	**Can we reduce the impact by taking different action?**	N/A	

1 Introduction

These Guidelines and Regulations apply to all IT facilities and resources on any Suffolk New College site and College equipment off-site, including open access and course-related and classroom-based facilities. The College takes very seriously misuse of IT facilities and resources and will take sanctions if any concerns are raised by internal or external parties.

The computer network is provided to support learning and teaching. Students may use a variety of software, make use of storage, scanning and printing facilities as well as interact and communicate with other people by sending and receiving messages. Students are responsible for their own actions in accessing and using the College's computer and e-learning resources. The use of the College's facilities is a privilege and not a right.

Open Access facilities are available in the Learning Curve.

Course-related facilities are available within teaching areas.

2 Scope

The Student IT Acceptable Use Policy applies to all users of Suffolk New College's computer network, and it applies to the use of any of the College's computers (including laptops, tablets, printers and mobile phones), wherever they are physically located. The Policy also applies whenever data is transmitted over the network via a privately-owned computer or device, wherever the machine is physically located. The Policy also covers use of the College's online services whether they are accessed from within the campus or from the internet.

3 Access to computer resources

The College IT resources are available for use by any student enrolled on a recognised course at Suffolk New College. Access to the College computers is controlled by personal username login. You will be provided with a user name, email address and password which you can use to logon to the College network. You must never give your password to anyone and you must never log on to a computer for someone else to use, or use another person's password. Valid users are responsible for all activity on their own user account, even if carried out by another person. Any user found to be using another person's username to gain access, will be subject to disciplinary action under the Supporting Student Achievement Policy. College management retains the right to ask for passwords or to reset them – this will be recorded at the IT Helpdesk for auditing purposes. All students must show a valid College ID card when asked to do so when using open-access IT facilities. Students are not allowed to lock their PC workstations and leave them unattended.

Computer use is monitored by the IT Services Team to determine appropriate use. Internet use is logged and recorded by the IT Services Team to enable follow up investigation of sites visited, files and emails if there is reason to suspect misuse of the network. Therefore, you should not expect that files or emails stored on the network will be private. Internet filtering software is installed to restrict access, as far as possible, to inappropriate or offensive websites and email filtering software is installed to reduce the amount of spam or junk mail. These are reviewed and updated regularly by commercial service providers, though there can be no guarantee that unsuitable material is never available to users.

If you open a webpage or receive an email that is offensive to you or others, racist, illegal, obscene, misleading, promotes extremism or if you are in any way unsure or suspicious about it, report it to a member of staff immediately.

4 Acceptable uses of IT resources

- To support your study or other College related work;
- Sending or receiving personal email;
- Recreational use, as long as it does not prevent others from using the computers for academic or College-related activity.

5 Unacceptable uses of IT resources

Anyone behaving in a manner likely to disrupt purposeful activities whilst teaching and learning using any IT resource may (at the discretion of a member of staff) have their access restricted using the College classroom management system.

6 The following are not permitted:

- Visiting internet sites, making, posting, uploading printing or passing on material or comments that contain or relate to: offensive or racist messages or images, obscene language, harassing or insulting others, pornographic (including child pornography), promotion of illegal acts, terrorism or promotion of extremism, gambling, knife and other forms of criminal violence, and drug abuse.

- Damage to computers, computer systems or computer networks, changing machine settings including desktop, printer or monitor settings.

- Uploading or downloading any unauthorised software, in particular hacking, malware, IT vulnerability exploitation or other system tools.

- Attempting to spread computer viruses or any other malicious software.

- Engaging in spamming or other bulk emailing.

- Internet chat, unless this forms part of a lesson supervised by a member of staff.

- Violation of copyright laws. This includes copying material from a website and passing it off as your own work.

- The downloading and/or distribution of music and video files for which licence fees have not been paid also constitutes an infringement of copyright, trademark and intellectual copyright, and is illegal.

- Attempting to load additional software, or attempting to tamper with the default settings for PC's on the College network. Software applications available to users are limited to those set out on the PC desktop and the start menu.

- The playing of software-based games, including those on or from the Internet, is not allowed, unless part of a supervised lesson.

- Inappropriate saving, to the network, of personal photos, music, video or other data.

- Inappropriate use of social media whereby information is communicated that brings the reputation of the College into disrepute.

- Recording, filming or photographing staff and other students without permission in advance.

7 Privately owned devices including laptops, netbooks, tablets and phones

All rules of usage for internet access and computer usage continue to apply. Students should ensure that their machines are properly protected against viruses.

The College cannot accept responsibility for any damage, howsoever caused, to computers or their contents as a result of being connected to the College network. It is the responsibility of the owner to ensure that there is a licence for all software installed on privately owned equipment. You will need to have your electrical equipment PAT tested by the College if you use our mains electricity supply or network portals. PAT tests are carried out by Facilities staff.

Inappropriate material accessed off-site should not be brought into College and shared with others.

Students should exercise care when communicating online or using social networking sites particularly in relation to the College and existing or past students or members of staff. Defamatory comments or inappropriate use of

materials, including text, video, photos and images, will be challenged and could lead to disciplinary action.

Mobile phones or other recording devices must not be used to record still or moving images or record sound on College premises or College related activities without the permission of a member of staff. If permission is gained, the recording is for the sole use of the student to support their learning and must not be used on any other platform. Mobile phones should not be used to send offensive messages which harass, insult or attack others.

Personal mobile phones or other devices must not be used to promote extremism or terrorism.

8 Sanctions

The College takes the rules set out in the Student IT Acceptable Use Policy very seriously. Any student breaking the rules may be subject to the Supporting Student Achievement Policy. In extreme cases legal action may be taken.

Incidents which appear to involve deliberate access to websites, newsgroups or online groups that contain the following materials will be reported to the Police:

- Images of child abuse (images of children apparently under 16 years of age) involved in sexual activity or posed to be sexually provocative;
- Adult material that potentially breaches the Obscene Publications Act;
- Criminally racist material in the UK;
- Promotion of extremism and terrorism;
- Any unauthorised access or use of College computing and/or network systems which is in violation of the Data Protection Act 2018 or the Computer Misuse Act may be subject to criminal prosecution.

9 Management and Monitoring

The College has software and systems in place to filter and record all Internet usage from College devices. These systems are capable of recording (for each and every user) each action performed. The filtering software used by the College can prevent access to many but not <u>all</u> inappropriate sites. The logging and recording of internet access can identify inappropriate use of the Internet.

The College reserves the right, as always, to inspect any and all files stored on computers in all areas of the network in order to assure compliance with policy. The College may also *review Internet activity and analyse usage patterns where there is cause to suspect inappropriate use.* Auditors (internal or external) have the right to access any computer files and systems in the performance of their duties.

The Learning Curve staff and teaching staff also use software to monitor student usage of the Internet. If a student finds him/her connected accidentally to a site that contains illegal, sexually explicit or offensive material, or any material that they were not expecting they must disconnect from that site immediately and inform a member of staff.

10 Review of Policy

The procedures in this Policy will be subject to on-going review and modification in order to keep up with advances in technology.