ASHTON
SIXTH FORM COLLEGE

Student Acceptable Use Policy

College Computer Network, e-mail and Internet

Last updated – May 2020

This policy applies to :	All students
Author/Department:	Head of IT & Learning Resources
Area/Person responsible:	Assistant Principal – Learning & Achievement
Date approved:	January 2018

Revision History

Version	Date	Responsible Person	Changes
Original	January 2018	John Haigh	
Rev 1 2019	January 2019	John Haigh	1) updated legislation references (section 5) 2) updated password requirements (section 2)
Rev 2	May 2020	John Haigh	1) updated responsibilities (page 1) 2) amended email standard notice wording (section 3, para 3.3.8) 3) moved section on Social Media (now section 4) 4) added section on working at home (section 5) 5) added section on Online Teaching & Learning (section 6) 6) renumbered section on Monitoring (now section 7) 7) amended legislation references and renumbered section (now section 8)

The Equality Act 2010: The Equality Duty

The College has a duty to consider the needs of all individuals in our day-to-day work – in shaping policy, in delivering services and in relation to our employees. The Equality Duty has three aims, which require the College to have due regard to the need to:

- **Eliminate unlawful discrimination**, harassment, victimisation and any other conduct prohibited by the Act;
- **Advance equality of opportunity** between people who share a protected characteristic and people who do not share it; and
- **Foster good relations** between people who share a protected characteristic and people who do not share it.

Does the policy support the aims of the Equality Duty?	**Yes**	x	**No**		**N/A**	

If no, complete a full equalities impact assessment (guidance and forms available on the intranet)

1 Introduction

1.1 The College provides Information and Computer Technology (ICT) facilities for use by its students and staff. In the interests of all users, any person using ICT facilities must abide by the College's Acceptable Use Policy (AUP).

2 Security

2.1 User Accounts

2.1.1 Only the named account user should use their account on the College computer network. The following password restrictions are in place:

- A minimum of 8 characters.
- Contain 3 of the following – uppercase, lowercase, numbers, special characters (e.g. !£@&)
- Inability to reuse any of the previous 5 passwords.

2.1.2 The owner of the account must take all reasonable steps to protect and maintain the security of any passwords allocated for their use. Specifically they should not:

- Disclose their passwords to anyone else.
- Allow anyone else to access a computer using his or her account.
- Log on to the network using another person's account.
- Leave a computer unattended without first logging off.

2.1.3 Account users who suspect the integrity of their password has been compromised should change it immediately and inform the IT Team.

2.2 Data Storage

2.2.1 All users are allocated a user 'home directory' in which to store their personal files. Users should not attempt to access directories and files for which they are not authorised. In particular, the confidentiality of data belonging to other users must be respected.

2.2.2 Because storage space is limited, users must save only essential files. In particular the downloading and saving of webpages is discouraged because these pages often contain large images which can bloat file sizes. The downloading of music and games files is not allowed. Any music or games found in students' folders will be removed by IT staff.

2.2.3 Disc quotas are in place to control and manage the storage space available and users will not be allowed to exceed this limit. It is the user's responsibility to ensure good house-keeping of their home directory by deleting unnecessary files and regularly emptying their Recycle Bin.

2.2.4 All students have a Microsoft Office365 account; while this has been implemented primarily for its e-mail facilities it also provides each user with 25GB of 'OneDrive for Business' storage. You should make full use of this resource; for example, storage of raw source image files for photography, etc.

2.3 Software

2.3.1 All software will be installed by IT staff. If any user requires software to be installed it should be forwarded to the IT helpdesk email address with the appropriate licence.

2.3.2 Users must not use the College's equipment to run any software other than that provided by the College on the particular machine. This includes music, videos, games or other software available via the Internet or other third parties.

2.3.3 Users must not attempt to install or uninstall any executable files on to, or from, a college computer.

2.3.4 Users must comply with their legal obligations concerning copyright. Under no circumstances may any of the equipment in college be used to make copies of software or other data without the authorisation of the copyright holder.

2.3.5 College runs Microsoft operating systems, Windows 10 and Microsoft Office 2016 (English versions) on all computers. Users who use other software at home may find incompatibilities with work created at home and then brought into college. IT staff will help if possible but cannot guarantee to resolve all incompatibility issues. Microsoft Office software is made available for home use to all college users and can be accessed via their Office365 account.

2.4 Viruses

2.4.1 Users must take all reasonable steps to exclude and avoid the spread of malicious software and must co-operate with measures instituted by the College to prevent the spread of such software.

2.4.2 All college computer equipment is protected against malicious software by up-to-date Microsoft System Centre Endpoint Protection software. All users are strongly advised to ensure that their home computers are protected with suitable anti-malware software.

2.5 Hardware

2.5.1 IT hardware must be treated with care and used only in accordance with its proper operating instructions. Problems with equipment should be reported to the IT helpdesk. Users must not move or remove equipment, unless designed for this purpose e.g. laptops, tablets.

2.5.2 Users may connect their own devices to the College network using the 'ASFC-BYOD Wireless Network'. Further information can be found on the Student VLE.

2.5.3 Users are encouraged to use the College's remote desktop to access college work remotely or use Microsoft OneDrive as 'cloud storage' which can be accessed from any browser enabled computer. It is permissible to use USB flash devices on college computers as memory storage; i.e. to store and transfer data, however, users are not permitted to run applications on the device while attached to the College network. Users should be aware that USB memory sticks have proven to be susceptible to damage and data corruption and should not be used for primary storage.

3 Internet access and e-mail

3.1 General Points

3.1.1 All College staff and students have access to the Internet and email. However, such widespread Internet and e-mail access opens up the College to risks and liabilities. It is therefore essential that all users read these guidelines and make themselves aware of the potential liabilities involved.

3.1.2 The use of the Internet and e-mail is primarily for college related purposes.

3.1.3 Computers and e-mail accounts are the property of the College and are designed to assist staff and students in the performance of their duties and studies. There is, therefore, no guarantee of privacy in any e-mail sent or received.

3.1.4 Inappropriate use of the Internet and e-mail is considered to be the downloading or transmitting of any material which might reasonably be considered to be pornographic, obscene, abusive, sexist, racist, extremist or defamatory. This includes content circulated in emails, regardless of the point of origin.

3.1.5 The use of chat rooms, bulletin boards and the accessing of web-sites of an inappropriate nature will be treated as serious breaches of this Policy. Such misuse of the computer systems will be treated by the College as misconduct. In all cases the College Safeguarding team will also be informed.

3.2 Use of the Internet

3.2.1 The sites accessed by users must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action.

3.2.2 The use of the Internet, e-mail and wireless access during 'out-of-hours' times such as breaks and lunchtimes is not regarded as different to its usage at any other times.

3.2.3 College has implemented a web-site blocking facility in order to restrict access to those web-sites deemed inappropriate. However, due to the international scale, the linked nature of information and the almost exponential growth of content available via the internet, it is not possible to guarantee that unsuitable material will never appear on a computer. The College cannot accept liability for the material accessed, or any consequences thereof.

3.2.4 In the event that distasteful or unacceptable materials do slip thorough the firewall then users should contact the IT helpdesk in order that the content can be blocked as a matter of urgency. Conversely, if any member of staff should come across a web resource that is blocked unnecessarily then they should also contact the IT helpdesk so that the resource may be investigated and unblocked if appropriate.

3.2.5 The accessing of websites of an inappropriate nature will be treated as serious breaches of this Policy. Such misuse of the computer systems will be treated by the college as misconduct and will, in certain circumstances, be treated as gross misconduct. The College reserves the right to use the content of any user's e-mail in any disciplinary process.

3.2.6 The accessing, or attempted access, of websites which are deemed to be extremist in nature or concerning online behaviours evidenced through the College web filtering system will be referred to the College Safeguarding team.

3.2.7 In accordance with the Prevent Duty web filters are in place to track and block any attempts to access websites linked to terrorism, extremism or radicalism.

3.2.8 The use of web-based proxy servers is not allowed. Any such use will be seen as an attempt to breach the College acceptable use policy and may lead to disciplinary action and may, in certain circumstances, be treated by the College as gross misconduct.

3.3 Compilation and Use of e-mail

3.3.1 E-mails should be drafted with care. Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from their computer.

3.3.2 Users should not make derogatory remarks in e-mails about staff, students, or any other person or organization. Any written derogatory remark may constitute libel.

3.3.3 Users must never hide the identity of the sender, impersonate any other person when using e-mail or amend messages received.

3.3.4 Users should not create e-mail congestion by sending trivial messages or unnecessarily copying e-mails.

3.3.5 Users should make hard copies of e-mails which they need to retain for record keeping purposes.

3.3.6 Reasonable, occasional personal use of e-mail is permitted but should not interfere with college work. The contents of personal e-mails must comply with the restrictions set out in these guidelines. Excessive private use of the e-mail system may lead to disciplinary action.

3.3.7 By sending e-mails on the College's system, users are consenting to the processing of any personal data contained within that e-mail. If users do not wish the College to process such data they should communicate it by other means.

3.3.8 All college e-mails are accompanied by the College's standard notice which currently states:
"This email and any files transmitted with it are confidential and intended solely for the use of the individual(s)to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of Stamford Park Trust. If you are not the intended recipient, be advised that you have received this email in error and that any use, dissemination, forwarding, printing or copying of this email and its contents is strictly prohibited. If you have received this email in error, please contact the sender. Stamford Park Trust, a company limited by guarantee registered in England and Wales, company registration number 11736886. Registered Office: Ashton Sixth Form College, Darnton Road, Ashton-under-Lyne, OL6 9RL"

3.3.9 The above conditions also apply to remote use of a college email account.

4 Social Media

4.1 Ashton Sixth Form College is keen to encourage innovation in the use of technology with students. Some staff may therefore use Social Media sites such as Facebook to enable contact with students outside of lessons. Students engaging in learning using Social Media must abide by the following:

4.1.1 Students will be invited to join the Social Media group of their particular subject. Requests to join will not be allowed.

4.1.2 Subject teachers will be administrators of Social Media groups. Students will not be permitted to have administration rights on Social Media groups.

4.1.3 Students must not do anything that could be considered discriminatory against, or bullying or harassment of, any individual, whilst a member of a College Social Media group, for example by:

- Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion, belief or age.
- Using Social Media to bully another individual.
- Posting images that are discriminatory or offensive, or links to such content.
- Posting images of college staff or student without consent.
- Bring the College into disrepute, for example by: Criticising or arguing with teachers or other students.
- Making defamatory comments about individuals or other organisations or groups.
- Posting images that are inappropriate or links to inappropriate content.

4.1.4 Breach copyright, for example by:

- Using someone else's images or written content without permission.
- Failing to give acknowledgement where permission has been given to reproduce something

4.1.5 Any student who has not accepted this agreement will not be permitted to join a college-badged Social Media group.

4.1.6 The college reserves the right to remove any student or member of staff from a college-badged Social Media group if any communication is deemed to be inappropriate.

5 IT Security & Home Learning

5.1 Introduction

5.1.1 Learning at home can be helpful in promoting flexibility for students, however this presents increased cyber security challenges that need to be managed.

5.1.2 In addition, cyber criminals may prey on users taking advantage of events such as the Covid-19 outbreak in 2020, and sending 'phishing' emails that try and trick users into clicking on a link to a rogue website (which could download malware onto their computer or steal passwords).

5.1.3 The college will provide support to students where possible remotely through the use of Canvas and other electronic resources. It is important to remember that the same college-related cyber security rules apply at home, this can sometimes be forgotten when working in a more familiar environment.

5.2 IT Equipment

5.2.1 Devices used for studying outside the college environment are more vulnerable to theft and loss. Whether using your own device or the college's, ensure it is secure and not left unattended. If the device is portable and not being used please keep it somewhere safe.

5.2.2 If you have loaned a college device and this is lost or stolen please report it as soon as possible to techsupport@asfc.ac.uk.

5.2.3 When studying from home it is more important than ever that you log out of any systems when you have finished using them. Cedar, Canvas etc are all web sites that can be accessed with your details so is crucial that you log out of the applications, especially on a shared device.

5.3 Software Updates

5.3.1 Please keep your desktop software and antivirus up to date on your home machines. If you are running Windows 10 there is a simple guide on how to do this here:https://support.microsoft.com/en-gb/help/4027667/windows-10-update

5.4 Password Rules

5.4.1 Attackers will try the most common passwords or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

5.4.2 Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.

5.4.3 Report attacks as soon as possible to techsupport@asfc.ac.uk - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.

5.4.4 Use strong passwords as cyber-attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

5.4.5 Use a separate password for your college account. If an online account gets compromised, you don't want the attacker to also know your college password.

5.4.6 Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.

5.5 Remote Desktop/Direct Access

5.5.1 The College will provide remote access to student data files through a Remote Desktop or via Direct Access when using a college issued device.

5.5.2 When using the Remote Desktop and Direct Access students are subject to the restrictions and conditions applied to internal network access.

5.5.3 In particular, students must ensure that they log out of Remote Desktop when using this at home on a shared device to ensure that the security of college systems is maintained.

6 Online Teaching and Learning

6.1 Ashton Sixth Form College will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

6.2 Students must ensure that they read and apply the guidance provided by the college relating to the delivery of online teaching, in particular in relation to the use of webcams and platforms such as MS Teams.

6.3 Staff will only use platforms specified by senior managers and approved by the Head of IT and Learning Resources to communicate with students (MS teams via the Canvas integration as the main platform).

7 Monitoring

7.1 Where the College has reasonable cause to believe that there is a breach of this Policy it has the right to monitor and inspect any and all aspects of its computer systems. This includes, but is not limited to; the abuse of Internet access, the transmission of virus infected files, the sending of unwanted, inappropriate or offensive e-mails, excessive use of personal e-mails.

7.2 College network users should be aware that all Internet access and usage is recorded; this information includes:

- User name
- Computer name
- Web page
- Date and time

7.3 Any website deemed to be inappropriate can and may be blocked from access within college.

7.4 The college reserves the right to use the content of any computer logs and records or any e-mail in any disciplinary process.

8 Legislation

- The Computer Misuse Act, 1994
- The Data Protection Act, 2018
- General Data Protection Regulation, 2018
- Regulation of Investigatory Power Act, 2000
- The Telecommunications Act, 1996
- The Copyright, Design and Patents Act, 1998
- The Human Rights Act, 2000
- JANET Guidelines