Acceptable Use Policy

1 - Introduction

All Staff and Students share the IT facilities at The Sixth Form Bolton. These facilities must be used responsibly by everyone on and off-site, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt College business and interfere with the work or rights of others. Therefore, all staff and students are expected to exercise responsible and ethical behaviour when using the College's Information Technology resources. Any action that may expose the College to risks of unauthorised access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including cessation of study programme.

This policy covers the following key aspects:

- College network
- Electronic Mail
- E-Safety

This policy applies to all staff and students at The Sixth Form Bolton and include on-site and off-site access. There are further policies that relate to students. Failure to adhere to this policy may result in disciplinary action.

1.1 - Usage of the College Network

The College network is defined as all personal computers (including laptops and tablets), printers and devices connected to the physical and wireless network and associated services, i.e. the Internet. This includes devices not owned by the College, i.e. contractor devices connected to the College's "AccessSFB" wireless network.

All users using devices falling within this definition must adhere to the following guidelines:

1.2 - General

- Users are responsible for the use, activity and compliance of their network account and associated services, i.e. Internet activity;
- Students should report any damage to college equipment as soon as its noticed.
- Any attempt to move, harm or destroy any network hardware or the data of another user will be considered as vandalism and is strictly prohibited;
- Users must not attach unauthorised hardware devices not approved by the College to the College network;
- Games are not permitted unless authorised by the Head of IT;
- The time period between 09:00 PM and 7:00 AM is considered a maintenance period and access to systems / services may be disrupted without prior notification. Users will be given prior notification of any maintenance taking place outside of these times;

Acceptable Use Policy

1.3 - Data security / allocation / retention

- Use of the network for any illegal activities, such as hacking, is strictly prohibited. It is gross misconduct, and a criminal offence under the terms of General Data Protection Regulation (GDPR) to disclose personal data to any person not authorised to receive it.
- Users will be allocated a proportion of the storage space on the Network appropriate to their role within the College and the availability of storage. Additional space may be made available at the discretion of the Head of IT and users may only use the network space allocated to them;
- No guarantee can be made by the College regarding the privacy or security of data held within individual user network accounts. This also applies to other associated services, i.e. email;
- The Head of IT has access to all accounts and messages, any inappropriate files, data or messages may result in the suspension of the network account and could lead to disciplinary action including dismissal;
- Users must not deliberately introduce any virus, worm, Trojan horse or any other "nuisance" program or file onto any system or take deliberate action to circumvent any precautions taken by the College to prevent "infection" of its machines;
- Users should not store sensitive data on local workstations or on portable devices such as USB pen drives. In line with the College's GDPR policy users are reminded to consider whether the storage of sensitive data is appropriate;
- If USB storage is needed to store data, it should be encrypted using Bit-Locker.
- The storage of copyrighted material, such as music and video files, is prohibited;
- Data stored on network shares will be backed up on a daily basis;
- The College electronic mail solution is facilitated by the Office 365 service. As such users are subject to the backup, storage and retention limitations as defined by the relevant subscription.
- Any data and emails that are no longer needed should be deleted.
- Activity on devices is monitored and logged.

1.4 - Your Account

Network Passwords

Do not use the same password for all your accounts. Use a different password for every account you set up.

When changing or setting your network password, it must meet the following requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least 12 characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)

- Non-alphabetic characters (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.

If you enter your password wrong 3 times, your account will be locked out for 30 minutes, after this time you can try again.

Password Resets

When you first log onto Office 365 you will be presented with a request for more information screen. Follow the instructions and set up either an authentication phone, alternative email address or answer a number of security questions and in the event you need to reset your password you will be able to do it via Office 365. If you don't set this up, you will need to come into College to reset your password.

Once set up simply click on '*forgotten my password*' on the sign in screen and then follow the onscreen instructions.

Office 365

The College gives users access to Office 365, which allows Staff and Students access to Email, Office web tools (Word, Excel and PowerPoint), Teams and OneDrive (Cloud Storage).

To access these resources, go to https://www.office.com and sign in with your College email address and password.

Your College email address will be in the following format:

ID Number@bolton-sfc.ac.uk

For example, 123456@bolton-sfc.ac.uk

2 - Internet Access

The College has implemented content filters to prohibit access to the following categories of sites:

- Intolerance;
- Malware & hacking;
- Online auctions;
- Plagiarism;
- Adult/Mature Sites;
- Terrorism;
- Games;
- Alcohol and tobacco;
- Child abuse;
- Drugs;

- Gambling;
- Violence;

Requests for access to the specific sites contained within these categories, for curriculum purposes, should be made via your tutor; All Internet usage is logged. The viewing of Internet sites containing pornography, racist or other inappropriate material is specifically banned when using College equipment;

2.1 - Monitoring

The monitoring of student network activity, i.e. internet, file stores and PC activity, will be routinely undertaken.

3 - Usage of Electronic Mail

The College Electronic Mail system is defined as the hardware, software and services the College provides to access and facilitate network accounts with an address ending in *"Bolton-sfc.ac.uk*". This includes access to College electronic mail from outside the College, i.e. staff or students accessing electronic mail from home. Usage of electronic mail falling within this definition must adhere to the following guidelines:

3.1 - General

- All e-mail and associated system resources are the property of The Sixth Form Bolton;
- Users are responsible for the usage, activity and compliance of their electronic mail account;
- Access to the "All Staff" and "All Student" distribution lists is restricted.
- Users may not:
    - Use the College electronic mail system to pursue the interest of other organisations beside The Sixth Form Bolton;
    - Use email for commercial solicitation;
    - Use email for the interests of groups of staff or students except for The Sixth Form Bolton business;
    - Use email to distribute hoaxes, chain letters, or advertisements; and/or send rude, obscene, racist or harassing messages or pictures; or propagate viruses, knowingly or maliciously. This list is not exhaustive, nor exclusive;
    - Users must not send, forward and/or reply to large distribution lists concerning College business;

3.2 - Data security / allocation / retention

Users are responsible for sharing their own mailbox features, i.e. Calendars and Inbox. IT Systems will not amend mailbox permissions unless specifically authorised to do so by the Head of IT & Estates for purposes of support;

Electronic mail is a record and therefore the management of electronic mail and the users of email must comply with all applicable legislation, regulations, policies and standards (e.g. GDPR). This includes complying with copyright and licence provisions with respect to both programs and data;

The College electronic mail solution is facilitated by the Office 365 service. As such users are subject to the backup, storage and retention limitations as defined by the relevant subscription.

Any emails that are no longer required should be deleted.

3.3 - Monitoring

By default, IT Systems staff are not granted administrative access to mailboxes. If access is needed to a specific mailbox it must be authorised by the Head of IT.

The monitoring of user's mailboxes will be routinely undertaken.

4 - Social Media

Social media is a useful tool and The Sixth Form Bolton understand that students communicate via sites such as Facebook and Instagram. However, there are also risks attached to the use of social media and students are expected to use it responsibly whilst connected to the College network whether this be on a college device or a personal device. All users must adhere to the following guidelines when accessing social media sites thought the college network or on college premises.

- Use of sexually explicit language or viewing, creation or sharing of sexually explicit imagery is not permitted nor advised from a safeguarding perspective.
- Verbally abusive or threatening language is not tolerated.
- Use of racist or extremist language which would directly contravene British and College values, as detailed in the Prevent strategy, is not permitted.
- Use of social media for the purposes of radicalisation or the expression of extremist views is not permitted.
- Communication with staff members unless on a College established social media site is not permitted. Any such communication instigated by staff members to a student's personal social media should be reported to safeguarding team.

Please be mindful of the following when using social media.

- Don't post anything on social media that you wouldn't want others to see. Remember what you post could impact on your future career.
- Don't be pressured into doing anything inappropriate on social media like posting photos or videos.
- Don't accept people as friends or engage in conversations on social media if you don't know the people you are communicating with, be aware of "stranger danger".

4.1 - General guidelines

Exercise caution when accessing personal social media sites in a public environment, e.g. a classroom or library.

If your social media profile lists that you are a student at the College, it should also state that any views expressed are your own and do not represent the College.

Set your profiles to "private" to ensure control over who is able to access / view your information.

Ensure conduct on sites could not be seen as detrimental to the College or bring the College into disrepute.

Be security conscious and take steps to protect yourself from identity theft, for example by restricting the amount of personal information given out. Social Media websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords.

Change your social media password often. IT Systems can provide advice concerning password security if required.

What you must do

You must report any requests you may receive through social media to post sexually explicit or offensive imagery online to the safeguarding team.

You must report to a safeguarding officer if you view any extremist or radical views expressed online.

You must report any personal communication staff may make with you via social media.

You must immediately tell a Safeguarding Officer if you receive offensive or inappropriate messages whilst at the College. This includes messages sent to your personal mobile phone;

You must immediately tell a teacher or your tutor if you think your network account has been tampered with;

You must ensure all emails sent using your College email address to external organisations are carefully written and authorised by your tutor before sending;

What you must not do

- You must not upload explicit or offensive imagery to social media sites.
- You must not use College network to express extremist or radical views.
- You must not communicate with staff via personal social media accounts, unless through a College established social media site such as a course specific Facebook site.
- You must not take or upload images of anybody staff or students.
- You must not discuss issues relating to staff or students at The Sixth Form Bolton which may bring the college into disrepute
- You must not make or receive mobile telephones calls or text message during lessons;
- You must not reveal personal details of yourself or others in e-mail communication, or arrange to meet anyone you have met electronically;
- You must not forward chain letters;
- You must not send abusive or inappropriate emails, text messages or in any other way participate in the misuse of technology;
- You must not publish personal details on public websites, i.e. Wiki's and Blogs.
- You must not publish comments that may be seen as offensive when using websites.

5 - General Guidelines

5.1 - General

Report any incidents of vandalism, abuse or malfunction to your teacher, tutor immediately;

Any damage to College Property must be paid for.

5.2 - Good practice

Users are encouraged to change their passwords on a regular basis to maintain the security of their accounts, the system will force you to change your password every 120 days;

Do not reveal your network password to anyone. Remember, you are responsible for the activity of any accounts or devices associated to you;

Do not leave your computer / laptop / tablet unattended whilst logged in;

5.3 - Electronic Mail

Any email message received which is intended for another person should be returned to the sender. All copies of the misdirected message should be deleted after it has been returned to the sender;

If an email message is sent to a distribution list, the recipient of the email should consider whether their response needs to go to all persons on the list or only to the originator;

Users should consider carefully the tone of any email as the absence of body language and tone can cause what was meant as a casual or humorous message to be taken other than intended;

Copying individuals into an email using the 'CC' facility is a good way to send your message to the main recipient while also sending someone else a copy at the same time, i.e. for information purposes. Be aware, however, that when you send a message to more than one address using the 'CC' field, both the original recipient and all the recipients of the copies can see all the email addresses in the 'TO' and 'CC' fields. Each person who receives the message will be able to see the addresses of everyone else who received it. This is particularly important when including external email addresses;

Try not to type your entire message in capital letters or boldface, the recipient may perceive this as 'shouting' and won't be able to tell which parts of the message are especially important;

Use the 'high importance' email feature sparingly, not all emails are urgent;

Don't configure your email client to request a 'read receipt' for every email you send;

5.4 - Laptop Usage

- Before using a College laptop report any damage to your teacher
- Before using your laptop ensure that you adopt a posture in which you can keep your wrists straight, your shoulders relaxed and your back supported, and in which you feel comfortable;
- While using your laptop place it on a desk or table, do not support the laptop on your lap because of the potential hazards of heat transfer;
- Take a short break at least once an hour;
- Rest your eyes frequently by looking at something far away or by closing them;
- Adjust the screen angle and height to reduce stretching your neck and to minimize the glare on the screen;
- If you're connecting your laptop to the mains ensure that the cables do not present a trip hazard;

6 - Responsibilities

User

Users are responsible for ensuring that their use of the outlined systems is appropriate and consistent with this policy. Users must comply with any additional instructions or regulations displayed alongside computing facilities;