BSix Brooke House Sixth Form College
Policy Document

IT acceptable use policy

Subject:	Use of IT resources
Date of Approval:	May 2018 (updated September 2020)
Effective Date:	May 2018
Review Date:	January 2021
Person Responsible:	Vice Principal Finance & Resources
Approved By:	Corporation
For Action By:	All Staff, Students and Stakeholders
For Information To:	All Staff, Students and Stakeholders

1. Overview

1.1 This policy is addressed to all students and staff members, temporary or permanent. It is available to parents on. This policy can be made available in large print or another accessible format if required. The policy takes into guidance issued by the Department for Education and various college e-safety and acceptable usage policies.

1.2 Information Systems play a major role in supporting the day to day activities of the College. The availability, confidentiality and the data integrity of the College's information systems are essential to the success of its academic and administrative activities.

1.3 The System Security Policies and associated Codes of Practice set out the responsibilities for ensuring the security of Information Systems within College and the procedures to be followed to safeguard the resources provided as well as the confidentiality and integrity of the information held thereon.

1.4 The policies apply to all staff and students of the College and all other users authorised by the College. They relate to their use of College-owned/leased/rented and on-loan facilities, to all private systems, owned/leased/rented/on-loan, when connected to the College network directly or indirectly, including remote and Wi-Fi network connections to all College-owned/licensed data/programs, be they on College or on private systems, and to all data/programs provided to BSix by sponsors or external agencies.

1.5 BSix Sixth Form College is committed to protecting its staff from illegal or damaging actions by individuals, either knowingly or unknowingly to the BSix IT Infrastructure. Including, the Email systems, Operating systems, Management Information Systems and other related systems

1.6 The College has an obligation to abide by all UK legislation. Of particular importance in this respect is the Computer Misuse Act 1990, The Regulation of Investigatory Powers Act 2000 and the Data Protection Act 2018. These policies satisfy the Data Protection Act's requirement for a formal statement of the College's security arrangements for personal data. The requirement for compliance devolves to all users, who may be held personally responsible for any breach of the legislation.

2. Purpose of this policy

2.1 This policy outlines the acceptable use of computer equipment at BSix Sixth Form College. The rules are in place to protect the Staff, students and BSix Sixth Form College against the inappropriate usage and exposure of BSix sixth form College to risks that include virus attacks, hackers, the compromise of electronic network/ data systems and services, and any legal issues.

2.2 Other objectives of this policy include:

i) To ensure that all of the College's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse

ii) To ensure that all users are aware of and fully comply with this Policy Statement and all associated policies and are aware of and work in accordance with the relevant Codes of Practice;

iii) To encourage Students to make good use of the educational opportunities presented by access to the internet and other electronic communications

iv) To safeguard and promote the welfare of Students by preventing "cyberbullying" and other forms of abuse

v) To minimise the risk of harm to the assets and reputation of the College

vi) To help Students take responsibility for their own e-safety

vii) To ensure that Students use technology safely and securely

viii) To ensure that all users are aware of and fully comply with the relevant UK and European Community legislation;

ix) To create throughout the College an awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security (IS);

x) To ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

2.3 The policy relates to the use of technology, including:

i) E-mail

ii) The internet

iii) Virtual Learning Environments

iv) Social networking or interactive websites/software/content management systems.

v) Instant messaging, chat rooms, blogs and message boards

vi) Gaming sites

vii) Mobile phones and Tablets (including PDA and similar devices)

viii) Webcams, video hosting sites

ix) Personal music players

x) Handheld game consoles

xi) Interactive Whiteboards

xii) Photographic or electronic equipment

2.4 It applies to the use of any of the above on BSix Sixth Form College premises and also to any use, whether on or off BSix Sixth Form College premises, which affects the welfare of other students or where the culture or reputation of the College are put at risk.

2.5 While BSix Sixth Form College network administration strives to provide a reasonable level of privacy, users should be aware that the data they create or store on the corporate systems remains the property of BSix Sixth Form College. Due to the requirement to protect the BSix Sixth Form College network, management cannot guarantee the confidentiality of information stored on any network device belonging to BSix Sixth Form College.

2.6 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.

2.7 For security and network maintenance purposes, authorised individuals within BSix Sixth Form College may monitor equipment, systems, data and network traffic at any time, per the BSix Sixth Form College Audit Policy.

2.8 BSix Sixth Form College reserves the right to audit and monitor networks and systems on a periodic basis to ensure compliance with this policy.

3. Prohibited Use

3.1 The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

3.2 Under no circumstances is an employee of The Sixth Form College, BSix authorised to engage in any activity that is illegal while utilising BSix Sixth Form College resources.

3.3 Anyone suspecting that there has been, or is likely to be, a breach of security should inform the Computing Support Manager immediately, who will advise the senior management on what action should be taken.

3.4 The list below is by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.5 The following activities are strictly prohibited

i) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use BSix Sixth Form College.

ii) Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographic material from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which BSix Sixth Form College or the end user does not have an authorised license is strictly prohibited.

iii) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

iv) Introduction of malicious programs into the BSix Sixth Form College network such as viruses, worms, Trojan horses, e-mail bombs, etc.

v) Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.

vi) Using a BSix Sixth Form College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

vii) Making fraudulent offers of products, items, or services originating from any BSix Sixth Form College account.

viii) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

ix) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

x) Port scanning or security scanning is expressly prohibited unless prior agreement from BSix Sixth Form College Computing Support Department is made.

xi) Circumventing user authentication or security of any host, network or account.

xii) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/ Intranet/ Extranet.

xiii) Providing information about, or lists of BSix Sixth Form College employees to parties outside the College.

3.6 Cyberbullying is deemed to be a misuse of digital technologies or communications to bully a person or a group, typically through messages or actions that are threatening and/or intended to cause offence, anxiety or humiliation.

3.7 This can Include but is not limited to

i) Abusive comments, rumours, gossip and threats made using digital communications and/or technologies – this includes internet trolling.

ii) Radicalisation or pressured suggestion

iii) Sharing pictures, videos or personal information without the consent of the owner and with the intent to cause harm or humiliation.

iv) Hacking into someone’s email, phone or online profiles to extract and share personal information, or to send harmful content while posing as that person.

v) Creating dedicated websites that intend to harm, make fun or spread malicious rumours.

vi) Blackmailing someone to do something they do not want to

4. Email Services

4.1 Electronic mail (e-mail) is an important means of communication, and it provides an efficient method of conducting much of the College's business. This document sets out the College's policy on the proper use of e-mail for College purposes. Assistance in compliance with this policy can be obtained from the following guidelines

4.2 Access to College e-mail is given to all staff, students, persons with honorary appointments, and approved third parties who agree to abide by College Policies, rules and regulations.

4.3 Staff and students are given access to e-mail systems for the conduct of College- related business. Incidental and occasional personal use of e-mail is permitted as long as it does not disrupt or distract the individual from the conduct of College business (e.g. due to volume, frequency or time expended) or restrict the use of those systems to other legitimate users.

4.4 Trade Union representatives who are members of the College may use the e-mail system to transact union business with their members.

4.5 Staff and students should ensure that e-mail is addressed to the correct recipient.

4.6 The College provides anti-virus and SPAM (unsolicited e-mail) filtering services to members of College using its Exchange e-mail service.

4.7 While efforts are made to keep these filtering services effective and up-to-date, the College can provide no guarantee that they will be effective against all viruses or SPAM. In cases where members of College experience distress caused by the receipt of offensive or excessive amounts of unsolicited e-mail, they may contact Computing Support for further guidance. Computing Support can limit an e-mail account to internal use only, or facilitate a change of e-mail address to alleviate the problem where requested.

4.8 All users are advised to use webmail, if necessary, to facilitate access to their e-mail files if they are likely to be absent from the College.

4.9 A central email gateway handles email entering and leaving the college. This gateway then communicates with all internal email servers. Email servers are a common source of security issues, and so all email will be handled by all central mail servers.

5. Staff and student non-engagement

5.1 Staff and students are prohibited from undertaking any of the following activities:

i) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

ii) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

iii) Unauthorized use, or forging, of email header information.

iv) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

v) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

vi) Use of unsolicited email originating from within BSix Sixth Form College networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by BSix Sixth Form College or connected via BSix Sixth Form College network.

vii) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.2 If a complaint is raised which alleges improper use of a College e-mail account, the Computing Support Manager (or delegated assignee) will carry out an initial investigation. If the complaint appears to have a reasonable basis, the matter will be referred to the appropriate part of the College so that further measures may be considered in accordance with College policy and regulations. Failure to comply with this e-mail policy could result in access to the facility being withdrawn or, in more serious cases, to disciplinary action being taken.

6. E-Safety

6.1 E-safety means limiting the risks that students and young people are exposed to when using technology, so that all technologies are used safely and securely.

7. Procedures

7.1 Students are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and lawful. Expulsion is the likely consequence for any Student found to be responsible for material on his or her own or another website that would be a serious breach of College rules in any other context. If you witness misuse by other Students talk to a teacher about it as soon as possible.

7.2 Students must not use their own or the College's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the enforcement guidelines of the College. If you think that you might have been bullied or if you think another person is being bullied, talk to a teacher about it as soon as possible.

7.3 If there is a suggestion that a student is at risk of abuse or you are worried about something that you have seen on the BSix Sixth Form College internet, talk to a teacher about it as soon as possible.

8. Enforcement

8.1 Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A copy of this Policy Statement will be given to all new members of staff by HR and to all new students by the Admissions office. Existing staff and students of the College authorised third parties and contractors given access to the College network will be advised of the existence of this policy statement and the availability of the associated policies, codes of practice and guidelines.

8.2 Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures as set out in the College policies for staff and College Regulations for students. Failure of a contractor to comply could lead to the cancellation of a contract. In certain circumstances, legal action may be taken.

9. Liability

9.1 Unless negligent under the terms of this policy, the College accepts no responsibility to the student or parents caused by or arising out of a Student's use of mobile phones, e-mail and the internet while at College.

9.2 E-mail and website addresses at the College may change from time to time.

10. Supporting Policies, Guidance Notes & Codes of practice

10.1 Supporting Policies amplifying this Policy Statement and Codes of Practice associated with these policies can be found on the College's website and on Teams. Staff, students and any third parties authorised to access the College Network to use the systems and facilities identified in this policy, are required to familiarize themselves with these and to work in accordance with them. Guidance Notes are also published to facilitate compliance.

11. Monitoring and review

11.1 All serious e-safety incidents will be logged on the appropriate College database. The Computing Support Department has responsibility for the implementation and annual review of this policy, in consultation with parents, Students and staff. The Computing Support Department will consider the record of e-safety incidents and new technologies. The Computing Support Department will consider and review the existing security procedures are adequate.