M1b ICT Acceptable Use of Technology for Students Policy

Scope

This policy is addressed to all students, and parents are encouraged to read it with their child. A copy of the policy is available to parents on request and the School actively promotes the participation of parents to help the School safeguard the welfare of students and promote the safe use of technology.

The School will take a wide and purposeful approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including but not limited to:

- the internet
- email
- mobile phones and smartphones
- desktops, laptops, netbooks, tablets
- personal music players
- devices with the capability for recording and/or storing still or moving images
- social networking and blogging
- instant messaging (including image and video messaging via apps such as Snapchat and
- WhatsApp), chat rooms, blogs and message boards
- webcams, video hosting sites (such as YouTube)
- gaming sites
- Virtual Learning Environments
- SMART boards
- other photographic or electronic equipment e.g. GoPro devices and drones.

This policy applies to the use of technology on School premises.

This policy also applies to the use of technology off School premises if the use involves students or any member of the School community, or where the culture or reputation of the School are put at risk.

Related Policies

- Behaviour Policy
- Anti-Bullying Policy
- Online Safety Policy
- Child Protection Policy

Aims

- The aims of this policy are:
  to educate and encourage students to make good use of the educational opportunities presented by access to technology;

- to safeguard and promote the welfare of students, in particular by anticipating and preventing the risks arising from:
    a. exposure to harmful or inappropriate material (such as pornographic, radicalisation, racist, extremist or offensive materials);
    b. the sharing of personal data, including images, videos and sounds;
    c. inappropriate online contact or conduct; and
    d. cyberbullying and other forms of abuse;
- to minimise the risk of harm to the assets and reputation of the School;
- to help students take responsibility for their own safe use of technology (i.e. limiting the risks that children and young people are exposed to when using technology);
- to ensure that students use technology safely and securely and are aware of both external and peer to peer risks when using technology;
- to prevent the unnecessary criminalisation of students.

Safe Use of Technology

We want students to enjoy using technology and to become knowledgeable users of online resources and media. We recognise that this is crucial for further education and careers.

The School will support students to develop their skills and make internet access as unrestricted as possible, whilst balancing the safety and welfare of students and the security of our systems. Students are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

Students may find the following resources helpful in keeping themselves safe online:

https://www.thinkuknow.co.uk/professionals/resources/
https://www.childline.org.uk/
https://www.ceop.police.uk/safety-centre/

Please see the School's Online Safety Policy for further information about the School's online safety strategy.

Internet and Email

The School provides internet access and an email system to students to support their academic progress and development.

All students will receive guidance on the use of the School's internet and email systems. The School email account is provided primarily to enable students to communicate with other members of the school community in an appropriate manner. If students are unsure about what constitutes appropriate use, they must seek assistance from a member of staff.

For the protection of all students, all incoming and outgoing electronic data will be monitored for inappropriate content by the School. Students should remember that even when electronic data has been downloaded and deleted, it can still be traced on the system. Students should not assume that files stored on servers or storage media are private.

School Rules

Students **must** comply with the rules and principles outlined in Appendix 1, which all students will be required to sign to confirm their understanding of and adherence to on an annual basis.

The purpose of these rules is to set out the principles which students must follow at all times to use technology safely and securely**. These principles and rules apply to all uses of technology.**

Procedures

Students are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be legal, safe, responsible and respectful to others. If students are aware of misuse by other students, they should report it to a member of staff as soon as possible.

Any misuse of technology by students will be dealt with under the School's Behaviour and Sanctions Policy.

Students must not use technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Bullying Policy. If students think that they have been bullied or that another person is being bullied, they should report it to a member of staff as soon as possible. See also the School's Anti-Bullying Policy.

In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's Child Protection Policy). If students are worried about something that they have seen on the internet, or on any electronic device, including on another person's electronic device, they must report it to a member of staff as soon as possible.

In a case where students are considered to be vulnerable to radicalisation they may be referred to the Channel programme. Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Dedicated Safeguarding Lead (DSL) and the IT Manager who will record the matter centrally.

Sanctions

Where a student breaches any of the School rules, practices or procedures set out in this policy or the appendices, the relevant houseparent or member of SLT will apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Behaviour and Sanctions Policy including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures, withdrawal of the right to access the School's internet and email facilities and/or detention. Any action taken will depend on the seriousness of the offence.

Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with our policies and procedures.

The School reserves the right to charge students or their parents for any costs incurred by the School as a result of a breach of this policy.

Monitoring and review

All serious safety incidents involving technology will be logged centrally by the DSL and the IT Manager.

The IT Manager is responsible for the effective operation of the School's network. They monitor the use of technology as set out in this policy and maintain the appropriate logs.

The SLT will review e-safety incidents and behaviour and take appropriate action as required.

Consideration of the effectiveness of the School's e-safety procedure will be included in the annual review of safeguarding for Governors.

Policy author / reviewer:	***Policy date / review date:***	***Next review due:***
Pastoral Team	8/1/2020	1/9/2020
T Burns	01/09/2020	01/09/2021
Adam Wroblewski	September 2021	September 2022
Adam Wroblewski	September 2022	September 2023
Adam Wroblewski	September 2023	September 2024

Acceptable Use of Technology Agreement

The School has the responsibility of providing you with safe, reliable and useful ICT resources that will help you to make the most of your learning opportunities. The School also allows you to bring your own mobile devices onto School premises. With these rights however, come the following responsibilities:

Access and Security

1. I understand that access to the internet from the School's devices and network is for educational purposes only.
2. I understand that I must not use the School's facilities or network for personal, social or non-educational use without the express, prior consent of a member of staff.
3. I will not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.
4. I understand that passwords protect the School's network and computer system. I will not let anyone else know my password. If I believe that someone knows my password, I will change it immediately.
5. I will not attempt to gain unauthorised access to anyone else's computer or to confidential information to which I am not authorised to access. If there is a problem with my passwords, I will speak to a member of staff or contact the IT Manager.
6. I will not attempt to access or share information about others without the permission of a member of staff. To do so may breach data protection legislation and laws relating to confidentiality.
7. I am aware that the School has a firewall, VLANS and Antivirus/Malware in place to ensure the safety and security of the School's networks. I will not attempt to disable, defeat or circumvent any of the School's security facilities. I will report any problems with the firewall to a member of staff or IT Manager.
8. I am aware that the School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of students. I will not try to bypass this filter.
9. I will not load material from any external storage device brought in from outside the School onto the School's systems, unless this has been authorised by the IT Manager.
10. I am aware that viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If I think or suspect that an attachment, or other downloadable material, might contain a virus, I will speak to the IT Manager before opening the attachment or downloading the material.
11. I will not disable or uninstall any anti-virus software on the School's computers.
12. I understand that methods for overcoming limitations placed on a school device such as ‘jailbreaking’ are treated with the upmost seriousness.

Use of the Internet

1. I will take care to protect personal and confidential information about myself and others when using the internet, even if information is obtained inadvertently. I will not put personal information about myself, for example my full name, address, date of birth or mobile number, online.
2. I will assume that all material on the internet is protected by copyright and such material

must be treated appropriately and in accordance with the owner's rights. I will not copy or plagiarise another's work.

3. I will not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, bullying, pornographic, defamatory or criminal in nature. I am aware that use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. I will tell a member of staff immediately if I have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.
4. I will not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.
5. I will not bring the School into disrepute through my use of the internet.

Use of Email

1. I understand that the School's email system is intended to support students in their academic progress and development. I know that all communications should be appropriate. I understand that examples of inappropriate communications are those which are abusive, racist, terrorist-related, sexist, homophobic, bullying, pornographic, defamatory or criminal, in nature. I will not send or forward trivial messages or jokes through the School's email system. I understand that not only could these cause distress to recipients (if considered to be inappropriate), but could also cause the School's network to suffer delays and / or damage.
2. I understand that all correspondence from my School email account will contain the School's disclaimer.
3. I will not read anyone else's emails without their consent.

Use of Mobile Electronic Devices

1. I understand that "mobile electronic device" includes but is not limited to mobile phones, smartphones, smart watches, tablets, laptops and MP3/MP4 players.
2. I understand that students in Years 7-11 may have limited access to their mobile phones, smartphones or smart watches during the normal academic school day (excluding break and lunchtimes).
3. I understand that use of mobile electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not I am in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use.
4. I understand that mobile electronic devices may be confiscated and searched in appropriate circumstances.
5. I understand that all mobile electronic devices are brought into school at my own risk. I understand that all devices should require a passcode or password to be unlocked and this should never be divulged to any other student.
6. I understand that the School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff, and I am aware that the school insurance does not cover the loss of mobile electronic devices.

Photographs and Images

1. I understand that using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
2. I understand that no photograph should be taken of any other student without their express permission.
3. I will only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.
4. I will allow staff access to images stored on mobile phones, cameras or devices and must delete images, if requested to do so.
5. I understand that the posting of images which is considered to be offensive or which brings the school into disrepute is a serious breach of discipline and will be subject to disciplinary procedures.
6. Sexting: I will not send indecent images of myself or others. I understand that doing so may constitute a criminal offence. If I commit such an act, it is likely that the local statutory authorities will be consulted and a school disciplinary sanction will be applied. Local statutory authorities include the Police Service and the Hertfordshire Safeguarding Children's Board, although this list is not exhaustive.
    a. I understand that once a photograph or message is sent, I have no control about how it is passed on. I may delete the image but it could have been saved or copied and may be shared by others.
    b. I understand that images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.
    c. If I am concerned about any image I have received, sent or forwarded or otherwise seen, I will speak to any member of staff for advice.

STUDENT NAME: _____

STUDENT SIGNATURE: _____

TUTOR GROUP: _____

DATE: _____