BURGESS HILL GIRLS

ICT Acceptable Use Policy: Students (Whole School including EYFS)	32d

Responsible for Initiating Review of Policy	SLT
Committee to Review	SLT
Last Review Date	March 2021
Review Period	2 years
Approved by (Committee and Date)	SLT March 2021
Approved by Board of Governors	April 2021
Effective Date of Policy	March 2021
Next Review Date	March 2023
Related Policies	Incorporating Use of Privately Owned Devices Policy 7a Safeguarding (Whole School) 9a Behaviour Policy (whole school) 10a Behaviour Policy: Bullying (Whole School)

1.0 Introduction

This Acceptable Use Policy (AUP) is to provide guidelines to ensure that you stay safe and act responsibly when using technology. By using technology in school or to work at home during periods of remote learning, you have agreed to follow these guidelines.

Network use and access are considered a school resource. If the school AUP is not adhered to, access will be withdrawn and appropriate sanctions imposed. The AUP should be read carefully to ensure the conditions of use are accepted and understood before it is signed.

2.0 Aims

The aims of this Acceptable Use Policy are:

- To encourage pupils to make lawful and appropriate use of the growing educational opportunities presented by access to the Internet, use of e-mail and other electronic communication.
- To involve the pupils in developing a code of practice for the use of the internet.
- To promote a culture that educates the pupils about the safe use of the internet rather than placing restrictions on access to particular sites.
- To enable the Head to safeguard and promote the welfare of pupils and to minimise the risk of harm to the assets and reputation of the School.
- To prevent abuse of e-mail and internet facilities available at the School.
- To ensure that the School is represented in all virtual public arenas in an accurate, fair and non-libellous manner.

3.0 Principles

- You may only use email and access the Internet once you have received appropriate training from a member of staff. If at any time after that, you are unsure whether you are doing the right thing, you must ask for help from a member of staff.

- You must do all you can to protect the security of the School's computer network, and the security of networks belonging to others. In particular, this means being aware of the possibility of computer viruses and taking sensible precautions to avoid bringing them onto our system or passing them to others.

- You must also try to protect personal and confidential information about yourself and others, even if you receive or come across this inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation.

- Cyber bullying is defined as bullying by 'the use of email, mobile phone/device and text messages, instant messaging, personal websites and/or chat rooms'. Any suspected cyber bullying (whether during school time or otherwise) will be managed under the School Policy on Bullying.

- You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of any computer system, or any information contained on such a system, including the School's system. This is known as "hacking" and is both a criminal offence and a serious breach of school discipline.

- You should assume that all material on the Internet is protected by copyright and you must treat

such material appropriately and in accordance with the owner's rights – you must not plagiarise another's work.

- Any message or attachment which **you** send whilst on the school network, or whilst using school-provided equipment, must be appropriate and courteous, and must not contain anything which is pornographic, violent, racist, sexist, discriminatory, defamatory or blasphemous. You may be acting unlawfully if it does. As far as you are able, you must also make sure that you do not search for or receive such material: it is your responsibility to reject it if you come across it, and inform a member of staff.

- You must not bring the School into disrepute through your use of e-mail and your access to the Internet.

- You must not enter into any contractual commitment, whether for yourself or on behalf of another (including the School).

- If using your own device within the school premises, the school expects that such a device contains age-appropriate content.

- Many devices feature camera and sound recording facilities. In the event that you wish to record an event within the school premises, it must be for educationally valid reasons, and it is essential that you seek the permission of a teacher beforehand. Covert recording is strictly prohibited.

4.0 Practice

A. General

1. The School's code of conduct is to be adhered to at all times. It is displayed in all tutor rooms and has been signed by all pupils.
2. You must not reset the settings on Web Browsers or any other software used to access the Internet or for use of e-mail.
3. No 'laptop' or other portable devices may be connected to the internal School network. Own devices can connect to the internet via the School's wireless infrastructure; refer to the Use of Privately Owned Devices Policy.
4. You must not load any software onto School computers – this includes Chinese or Cyrillic character sets, ICQ software, Kazaa, Gator, etc., so as to safeguard the School network from viruses and other risks to computer security.
5. You must not change the settings on any School computer unless instructed to do so by a member of staff. If you change the language on a computer during an MFL lesson, change it back at the end of the lesson.
6. Do not print unless the work is needed to hand in, there should be no printing of web pages unless needed for research, and generally it is better to bookmark the page.

B. Security and Privacy

1. Always log into the systems using your own username and password (unless specifically instructed to use different credentials by a member of staff).
2. Always keep your password secret; if you think someone else knows your password, reset it immediately.
3. Change passwords at regular intervals. Should you suspect your network/Google or any other BHG credentials to be compromised, you must change your password and inform ICT Support

immediately.

4. Passwords should be complex, be at least 8 characters and they should contain at least one letter and one number.
5. Always log out when you have completed your work session, this includes your Google account or app accounts on portable devices e.g. iPad.
6. Do not save your login credentials when using public machines or portable devices.
7. Always set a Pin Code/password for your mobile device.
8. If you lose your device that you use to connect to School systems e.g. google, report its loss to IT Support and change your passwords immediately. Report any unusual activity (for example, altered files etc.) to IT Support.
9. Do not attempt to bypass or alter security settings put in place on the BHG networks. They are there to protect you, your work and school resources.

C. Email

1. It is the expectation that you check your school gmail account once every school day; similarly staff will check their email account once every school day and respond appropriately.
2. You must not use the email facility during lessons unless instructed to do so by a member of staff.
3. If you think or suspect that an attachment sent to you, or other material that you want to download, might contain a virus, you must not open the attachment or download the material without first speaking to a member of IT Support to arrange a virus check.
4. You must not send or receive encrypted messages. If you receive any encrypted messages these must be referred to a member of IT Support.
5. The use of strong language, swearing or aggressive behaviour will not be permitted.
6. Emails containing material with violent, dangerous, racist, or inappropriate content must be reported to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
7. Email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities.

D. Internet Use

1. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else.
2. When online, users should not do anything that by-passes the School's Internet filtering system, for example by using Internet proxy sites.
3. Any comment or pictures added to social networking sites should adhere to the School behaviour rules that require pupils to be responsible, thoughtful and considerate.
4. Ensure you protect your personal reputation by thinking carefully before posting information online. Anything you post online is potentially public and permanent. Burgess Hill Girls does have a social networking presence in the form of Facebook, Twitter and Instagram accounts, and may in the future adopt other social networking profiles. If students are in any way linked to such presences it is essential to remember that communications within this arena fairly represents the School. Any form of communication via social networking tools should be for educationally valid purposes.
5. To preserve the Internet bandwidth needed by all in our community, and for security reasons, the following applies to all pupils:

    - No file sharing activity (e.g. Kazaa, WinMX, BitTorrent, Limewire). (It should be noted that this sort of file sharing is illegal)
    - No use of online gaming sites
    - Online gambling sites are strictly prohibited

- Online sites in which photos or other content can be anonymously shared need to be educationally valid, and prior permission from a teacher needs to be sought before using them
- Any activity that involves the downloading of large files or results in high levels of Internet traffic should be avoided

Please note that video and audio streaming uses a lot of Internet bandwidth and such use should be used only for education purposes, unless agreed by a member of staff.

E. Remote Access (via Remote Desktop Server)

1. All connections to the School's remote access site (via Remote Desktop Server) are monitored.
2. Users are expected to use Remote Access in a secure and responsible manner at all times.
3. Pupils should use Google Classroom in accordance with the instructions issued by members of staff.

F. Mobile Devices

1. Unless otherwise instructed by a member of staff, mobile devices should be switched off, or on silent, during lessons or at any time when asked to do so by a member of staff.
2. Mobile devices are not to be used in corridors or in the Dining Room during meal times.
3. **Under no circumstances should girls take photographs or videos using their mobile devices unless they have the express permission of a member of staff.**
4. Mobile devices should not be left in school bags or blazer pockets which are left unattended. It is recommended that Mobile devices are kept in lockers when not being used, either switched off or on silent mode.
5. It is recommended that mobile devices are named (indelible ink is also an option) and are brought into school at a pupil's own risk.
6. If there is an emergency which requires communication with home, pupils must speak to a member of staff who will deal with the matter. Parents/carers should only contact pupils at break time or lunchtime. In an emergency parents/carers should telephone reception and a message will be taken to the pupil. This ensures that a pupil is given support and privacy in dealing with a potentially difficult situation.
7. Pupils who feel unwell must always contact home via the school Nurse and not use their mobile device. This allows support and supervision and also avoids pupils leaving the school without a record being made.
8. Mobile devices cannot, under any circumstances, be taken into examination rooms. Breach of this rule will lead to invalidation of that examination and potentially other examinations.

5.0 Use of Privately Owned Devices (BYOD)

There are an increasing number of students who wish to use their own devices at the School and/or on the School network. These notes set out the basic requirements before a personal device computer may be used in this way.

1. Privately owned devices are brought onto School premises at their owner's risk. The owner is responsible for the security, storage and insurance risks beyond the School's insurance liability.

Similarly, any technical problems arising with the device computer are the responsibility of the owner. IT technical staff may be able to recommend action to take in case of difficulty, but the responsibility for repair and maintenance is with the device owner.

2. Before any device is used in School or a boarding house, it has to be subject to an electrical check by the School maintenance staff.

   If there is no requirement to access the School network or plug in the device then it may be freely used. However, students are strongly advised to install an up-to-date virus checker on any notebook computer or laptop they might use privately.

3. You must ensure that your device has sufficient battery charge for the day, at present there are no charging facilities on site.

4. **Always set a Pin Code/password for your personal device**. If you lose your device that you use to connect to School systems e.g. Google, report its loss to the IT Support team and change your passwords immediately. Report any unusual activity (for example, altered files etc.) to IT Support.

5. You will require a wireless enabled device to connect to the BYOD network. An information sheet including security passwords will be available on request from IT Support. The Current security system is WPA2 PSK and the password will be updated each term.

6. If the MS Office suite is not already available on your computer, students can obtain a license of Office 365 by registering with Microsoft. The alternative is to use Remote Desktop Server to provide access to selected software including MS Office suite.

7. Any software supplied by the School must be uninstalled from the computer on ceasing to attend the School.

8. The School network is protected by Firewalls and regularly updated virus protection. Internet access is filtered not only to prevent, as far as possible, access to websites with inappropriate content, and to ensure Internet access is freely available during the School day for educational use. Boarders using their own laptops on the student wireless network will be protected and content managed by the School's firewall but they are responsible for making sure they have up to date virus protection software installed on their computers.

9. The School's protocols and policy with regard to the use of e-mail and the Internet apply in respect of privately owned devices when used on School premises. All users should familiarize themselves with the School's ICT Acceptable Use Policy.

b. Use of Privately Owned Devices in lessons

10. If you would like to use your own device in lessons you need to speak to your teacher; your teacher is responsible for managing the teaching and learning within the lesson and will advise on appropriate use.

11. Your teacher will at times suggest that you may use your own device to supplement your learning. Your teacher cannot however advise on technical issues to do with your personal device.

12. Your teacher will arrange for appropriate facilities, e.g. booking laptops, to be available for all students where whole class activities require the use of technology.

6.0 Sanctions

- You will be liable to disciplinary sanctions including, in the most serious cases, permanent exclusion, if you breach this Protocol. You (or your parents) may also be asked to pay for any significant expenditure, or indemnify any significant liability, incurred by the School as a result of the breach.
- For your own protection and that of others, your use of email, the Internet and general computer use will be monitored by the School. Remember that even once you have deleted an email or something you have downloaded; it can still be traced on the system. We currently use Securus to monitor the school network.

7.0 Supervision & Monitoring

- All access to the Internet is filtered and managed, not only to prevent, as far as possible, access to undesirable material, but also to ensure network resources are available for educational use during the school day.
- The School Network Administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use and disclose any data found on the School's information networks in order to further the health, safety, discipline, or security of any pupil or other person, or to protect property. They may also use this information to inform the Head of any matter that constitutes a breach of the Behavior Policy.

This Policy should be read in conjunction with: Use of Privately Owned Devices Policy, Behaviour Policy: General Statement, Behaviour Policy: Bullying, Behaviour Policy: Pupil Discipline and Exclusion Policy

BURGESS HILL GIRLS

Pupil

As a user of the School's computer network and services, I have read the ICT Acceptable Use Policy. I agree to comply with the School rules contained within the policy. I will use the School's computer network and services in a responsible way and observe all the terms and conditions set out by our internet service provider.

Pupil's name: ……..……..

Pupil's signature……. Date: ……..

Parent/Guardian

As the parents or legal guardian of the pupil signing above, I grant permission for my daughter to use the School's local computer network and services, and a variety of cloud-based services such as the school Google Apps for Education domain. I understand that pupils will be held accountable for their own actions. I also understand that some material on the internet may be objectionable and I accept responsibility for setting standards for my daughter to follow when selecting, sharing and exploring information and media.

Parent's/Guardian's name:……..

Parent's/Guardian's signature……..…. Date: ……..……..

The register based upon the completed forms returned to the School is in operation from September 2013

Please note that this policy is subject to regular review and resubmission due to the fast pace of change in technological developments.