ACCEPTABLE MEDIA USE

AND BYOD POLICY

THIS POLICY IS REVIEWED ON AN ANNUAL BASIS

Policy reviewed by: Andrew Greenway - Director of Integrated Learning and Technology

Policy approved by: Robert Berry – Director of Operations

Review date: 01/07/2021

Submission: 01/07/2021

Version: v4.0

Policy actioned from: January 2021

Next review date: 31/08/2022

Reviewer's Signature: 

Approver's Signature: 

1. Purpose

1.1 Hall School Wimbledon Acceptable Media Use and BYOD Policy has been drawn up to provide safe use and protect all parties where ICT and media is in use. It is intended to allow all users safe access to computers, the Internet, email and electronic devices for educational purposes. Hall School Wimbledon embraces new technologies and wishes to develop student skills in this arena for lifelong use, but within the safety of the agreed usage policy.

1.2 Bring Your Own Device (BYOD) Policy applies to all staff and students. Mobile technology has become an integral part of modern life. It offers a valuable resource for use in the classroom and has numerous educational purposes. Educational purposes include, but do not exclusively cover, individual research, lesson preparation, project work, controlled assessment tasks, work storage, homework assignments, private study and communication with teachers and other students.

2. Rationale

2.1 Throughout this policy, the word 'device' is used to describe any mobile phone, tablet computer, laptop, or other device capable of communicating with either the Internet or mobile telephone networks and taking visual or sound recordings. Well-known examples of these that are likely to be owned by staff and students include iPhones, iPads and laptop computers.

2.2 This policy covers the use of and liability for all devices within the School and School grounds, on school trips, school sporting fixtures and is in addition to the current acceptable network usage policy for devices provided by school.

3. Legislative Framework

3.1 The policy covers all staff and students in the school and also third parties who have access to the School's electronic communication and network systems.

3.2 The use of the School's network systems and personal devices by students within school time is likely to involve the processing of personal data and is regulated by the Data Protection Act 1998, together with the Employment Practices Data Protection Code, issued by the Information Commissioner. The School is also required to comply with the Regulation of the Investigatory Powers Act 2000, the Telecommunications Regulations 2000 and the principles of the European Convention on Human Rights incorporated into the United Kingdom law by the Human Rights Act 1998.

4. Principles for Use

4.1 The School's Governing Body has overall responsibility for this policy, but has delegated day to- day responsibility for overseeing and implementing action to the Head or his representative.

4.2 The school's staff and students are expected to have regard to this policy at all times to protect its electronic communication systems from unauthorised access and harm.

4.3 The objective of this policy is to define the standards of conduct when employing the use of non-school owned electronic devices such as laptops, tablets, smartphones and other equipment used to access the internet and school learning resources.

4.4 Students who wish to bring their own device to school must submit a completed BYOD contract to the School.

4.5 The school reserves the right to refuse to allow access to particular devices or uses where it considers there is a risk to the school network.

4.6 Breaches of this policy will be taken seriously and any students found guilty may be subject to disciplinary action, in line with the school's behaviour policy. Students should not, under any circumstances, access our network resources without completing a BYOD Contract.

4.7 Use of personal BYOD devices is at the discretion of the School and should not be seen as a right. Students' own devices can be used in the classroom only at the teacher's discretion.

5. Equality of Opportunity

5.1 Any student who chooses not to bring their own device into school will be disadvantaged. Where necessary, school will provide devices to support curriculum activities and / or examination requirements.

6. Acceptable Use of User Owned Devices

6.1 The primary purpose of personal devices at school is educational or related to educational experiences. Use of personal devices during the school day is at the discretion of the staff. Pupils must use devices only as directed by their teachers. This will be signalled by a BYOD card mounted on the classroom whiteboard.

6.2 All BYOD devices shall only contact the Internet and local area network via the school wireless network. All internet access via the network is logged.

6.3 The use of cellular data (e.g. GPRS, EDGE, 3G, 4G, 5G etc) to access the Internet in School by students is strictly prohibited. All access must be by the school wireless network which is appropriately filtered. It is a condition of BYOD use under this policy that students are responsible for disabling cellular data on their device when on the School site.

6.4 The use of device camera or microphone functions on school premises, including school events, functions and visits, is prohibited unless approved by a staff member. Pictures, video or sound recordings taken in school may only be used in school related learning and must not be posted, uploaded or shared on any website or system (e.g. social media) other than one that belongs to or is approved of by school. We would highly recommend that any school-related media is stored on the school system.

6.5 Is it prohibited to use any device to take pictures, video, sound recordings of any student or staff member without their permission. Failure to comply will be a disciplinary matter.

6.6 When on the school site and switched on, all BYODs must be set to silent. Charging devices of any kind may only be used in school with the permission of a member of staff. If a student is found to be using an electrical outlet for charging their device without permission, then the charging device may be removed and can be collected at the end of the school day.

6.7 It is the students' responsibility to keep their device safe while at school, on school related visits and school sponsored activities.

6.8 The school provides limited technical support (mainly for networking connectivity issues) for BYOD equipment. Users should be competent in the use of their own device. The school does not, at present, provide direct printing from users' own devices.

7. Unacceptable Use

7.1 The downloading of any apps not provided by/distributed by the school whilst using our wireless network is undertaken at the owner's risk. The school has no liability for any consequent loss of data or damage to the individual's device.

7.2 Devices must not be used in a manner that would portray the School in an unfavourable light.

7.3 Devices should not be used to intimidate, abuse or share information that might be perceived as unfavourable against any member of staff, student or any person associated with the school.

7.4 Devices must not be used to share any information of an indiscrete or sexual nature with any other person.

7.5 Students are not permitted to use any device to create a wireless hotspot.

8. Security of Systems and Data

8.1 The BYOD policy and student contract for January 2021 onwards will be limited to access to the internet through the school's wireless network provision.

8.2 This policy gives permission for Students to use BYODs under the provision of this policy with subject teacher permission during time.

8.3 The school requires that students have installed anti-virus software, where available, for their device. The school does not guarantee provision of anti-virus software for BYOD.

8.4 Where students uses their own device to access and store data that relates to Hall School Wimbledon, it is their responsibility to familiarise themselves with the devices sufficiently in order to keep the data secure. This includes preventing theft and loss of data, keeping information confidential and maintaining the integrity of data and information. Students should delete sensitive emails once they have finished with them and delete copies of attachments to emails on their own device as soon as they have finished with them. In the event of loss or theft, a student should change the passwords to all the school's services accessed from that device and report the loss or theft within 48 hours to the Head.

8.5 When a device has been registered by the school and approved, the device can be connected to the school network via access with the wireless password for BYOD. Students will be able to use their own school login and are not permitted to share this access key or password with anybody else. If a student is found to have given this access key to anybody, their access to the system will be revoked and disciplinary action taken. The student's device will be issued with a monitored IP address. Students are not permitted to edit, adjust, disguise or share the IP address they have been given.

9. Monitoring of User Owned Devices

9.1 The school will not explicitly monitor the content of user owned devices, but reserves the right to monitor any traffic over the school system to prevent threats to the school network systems.

9.2 The school does not collect or store any passwords or personal information when a BYOD is connected to the internet.

9.3 The school may require access to a student's personal device whilst investigating cases of policy breach including, but not limited to, finding or retrieving lost messages lost due to computer failure, to assist in the investigation of wrongful acts including cyber bullying, hacking of the school's computer system, virus attack or to comply with any legal obligation.

9.4 The Head may require access to a student's personal device whilst investigating any behaviour or allegation relating to our School Anti-Bullying Policy. In these circumstances every effort will be made to ensure that the school does not access private information of the students which does not relate to the investigatory matter.

9.5 Controlled assessment on User Devices should only be carried out under direct instruction from a Teacher. Controlled assessment procedures and policies apply to all work completed on a user device. Students must seek specific permission from subject staff to complete any controlled assessment on a personal device. OFQUAL policies, contract and guidelines apply to all coursework completed on any device.

10. Protection of Devices

10.1 Users are required to protect their own devices e.g. with the use of password or PIN as appropriate. Students are responsible for the use of their own device while on the school site.

11. Theft, Damage and Insurance

11.1 The school takes no responsibility for any damage, loss, malware, theft, or insurance of any device that is not the property of the school, used within the school premises, including any event which causes the device not to function. We will investigate the theft, but not the loss of a device. If a device is stolen or damaged while on school premises, it is to be reported to student services immediately, in order that the incident can be logged.

11.2 It is the students'/parents' responsibility to ensure that they have sufficient personal insurance to adequately cover the device for any such occurrence. Any other costs, including the

download of data, incurred while using devices, are not chargeable against the school and are the sole responsibility of the owner.

12. Incidents and Response

12.1 Where a security incident involving students using their own devices arises at school, this matter will be dealt with seriously. The school will act immediately to prevent, as far as reasonably possible, any further harm occurring. The Head and School IT service provider will decide on the most appropriate course of action.

12.2 The School reserves the right to remove a device at any time if a student is seen to be violating this policy or any other related school policy.

13. Acceptable Media Use Policy Statement

13.1 Hall School Wimbledon has invested significant resources to provide computers, laptops and associated network technology for students. We invest significant resources in ensuring that our Wi-Fi and wired networks provide the best service that we can to aid student learning.

13.2 From January 2021, the school intends to develop opportunities for students to bring their own devices to assist their learning. This can include tablet devices and laptops and electronic notebooks to provide access to the Internet and word processing and other electronic documentation.

13.3 All students are expected to sign a contract agreeing a set of rules relating to behaviour covering the use of School IT or BYOD and to use of the Internet, privacy of work files, passwords and security. Students will be required to commit to this agreement prior to using IT or BYOD facilities. Any user of IT or BYOD facilities breaking the agreed rules will have their access restricted or removed for a fixed period of time.

Appendix 1

HALL SCHOOL WIMBLEDON

Acceptable Media Use Bring Your Own Device (BYOD) Contract

Name _____ Class_____ Device: ……

I agree to the following rules in relation to the use of IT in school:

- I will keep all usernames and passwords safe and secure.
- I will not use anyone else's user account.
- I will not eat or drink in any IT suite or classroom.
- I will not access any explicit or inappropriate material in school or use any game sites or websites that have been banned.
- I will use only computers or devices that the teacher has assigned to me or given me permission to use and will follow the teacher's instructions at all times.
- I will not send, store or publish any material on or through the school network which is bullying, threatening, abusive, indecent or offensive.
- I understand that use of unapproved sites will lead to me being barred from using the Internet and continual misuse may lead to me being banned from the school network.
- I understand that I will be expected to pay for any damage of equipment that I cause by misuse.

'Bring your own' [BYO] devices.

- I will only use my own device when permission has been given by a member of staff.
- I will only use the school network to access the Internet from my own device.
- I will not record, send on or store any pictures, video or sound of any other person without their express permission.
- I will ensure that my BYO device is always set to 'silent' when switched on.
- I will not charge my device in school unless given permission by a member of staff.
- I will not use my device to download any materials that are not directly for school work-related purposes.
- I understand that the safety of my device and all associated passwords is my own responsibility.
- I understand that the school will investigate theft or malicious damage to my device, but I am responsible for any accidental damage or loss of my device and any cost of repairs or replacement for it.
- I understand that the school will not provide technical support for my device and that there is no guarantee that the school's network will support my device.
- I understand that the school may require access to my device whilst investigating cases of inappropriate behaviour such as cyber bullying, hacking the school's computer system or spreading viruses or any other action relating to the school's anti-bullying policy.
- I understand that my device may be confiscated for 24 hours, in the first instance, if I break the rules explained to me.

I wish to use a personal device at Hall School Wimbledon for educational purposes. I have read and understood the BYOD Policy and agree to abide by its conditions. I understand that misuse of a device may lead to the device being confiscated for return to parents and that I may lose the privilege to bring a device into school in the future.

Signed _____ Student _____Date

Signed _____ Parent _____Date

Interpretation

In this policy, the term "senior manager" means a School Head and their designated deputies.

This policy applies to all employees in all Schools (save for Schools with their own procedure which shall prevail) and other work environments within Chatsworth Schools

This policy applies within all companies, which are wholly owned subsidiaries of Chatsworth Schools Ltd, a company registered in England, registered number 11552579.

The registered office of all companies is Crimea Office, The Great Tew Estate, Great Tew, Chipping Norton, Oxfordshire, OX7 4AH. Any enquiries regarding the application of this policy should be addressed to the Director of Operations at the above address.

POLICY AMENDMENT PAGE

Date	Key Amendments	Version Number	Signed off by
08/01/2021	Policy Approved – Fit for use by schools.	v3.0	RNB
01/07/2021	Policy updated	v4.0	AG