Acceptable Use Policy – Students

Please read this document carefully and discuss with your child

Policy Type	Statutory
Reviewed by	Deputy Head Pastoral Director of IT
Last Review	Autumn 2025
Next Review	Autumn 2026

1 Background

Haberdashers' Aske's Elstree Schools Limited, which includes Haberdashers' Boys' School and Haberdashers' Girls' School ("the School"), is committed to protecting its employees, Students and the wider School community from harm while using the School's IT systems.

IT systems are provided to enhance the quality of education provided at the School both directly in the form of teaching and open learning and in the form of administrative tools.

Parents are encouraged to read this policy with their child. 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 aims of this policy are as follows:

- to encourage active participation and support of every Student who accesses information and/or information systems
- 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:
    - exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials)
    - sharing of personal data, including images
    - inappropriate online contact or conduct; and,
    - cyberbullying and other forms of abuse.

- to minimise the risk of harm to the assets and reputation of the School
- to ensure that Students use technology safely and securely and are aware of both external and child-on-child risks when using technology
- to help all users take responsibility for their own safe use of technology; and
- to prevent the inappropriate use of hardware and software which may expose the School to risks including virus attacks, compromise of network systems and services and legal issues.

2 Related Policies and Useful Links

This Policy should be read in conjunction with the following other policies:

Academic Integrity Policy
AI Policy
Anti-Bullying Policy
Behaviour, Rewards and Sanctions Policy
Data Protection Policy
e-Safety Policy
Mobile Phone Guidance
Privacy Notices
Safeguarding Policy

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

- http://www.thinkuknow.co.uk/
- http://www.childnet.com/young-people
- https://www.saferinternet.org.uk/advice-centre/young-people
- https://www.disrespectnobody.co.uk/
- http://www.safetynetkids.org.uk/
- http://www.childline.org.uk/Pages/Home.aspx

3 Terminology

BYOD means Bring Your Own Device where Students are typically allowed to use their own laptop or tablet devices in School. We do not operate a BYOD service at Habs. Students may only bring in their mobile phone to school.

School Device refers to a school issued laptop or tablet computer, including desktop computers found in IT suites.

Personal Devices include laptops, mobile phones, wearable technology, tablets, iPods, MP3 players, and games consoles.

Wearable technology includes, but not limited to:

- Smartwatches (e.g. Apple Watch, Samsung Galaxy Watch)
- Fitness trackers (e.g. Fitbit, Garmin)
- Smart glasses (e.g. Google Glass, Ray-Ban Meta)
- Wearable audio devices (e.g. earbuds with assistant functions, bone-conduction headphones)
- Wearable cameras or microphones
- Augmented Reality (AR) or Virtual Reality (VR) headsets

Head, where not explicitly defined, means the Headmaster of the Boys' School or/and the Headmistress of the Girls' School.

Parents includes one or both parents, a legal guardian, or education guardian.

School means Haberdashers' Boys' School and/or Haberdashers' Girls' School which are operated by the Haberdashers' Aske's Elstree Schools Limited, the Schools Trustee of Haberdashers' Aske's Charity.

Student or **Students** means any Student or Students in the School at any age.

Technology means all computing and communications devices, network hardware and software, and services and applications associated with them including:

- the internet
- email and school messaging platforms including Microsoft Teams
- mobile phones and smartphones
- smart watches
- desktops, laptops, netbooks, tablets / phablets
- personal music players
- devices with the capability for recording and / or storing still or moving images
- social networking, micro blogging, and other interactive websites
- 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, audio recorders.

4 General Use and Ownership

Everyone should be aware that the data they create on the Schools' systems remain the property of the School.

Students are responsible for exercising good judgment regarding the reasonableness of personal use. For any guidance, please refer to a teacher or Head of Year/Section.

We want Students to enjoy using technology and to become skilled 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. The safe use of technology is integral to the School's curriculum. Students are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

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

5 Acceptable Use Guidelines

5.1 General

- Students are always responsible for their actions, conduct and behaviour when using technology. Use of technology should be safe, responsible, and respectful to others and the law. If a Student is aware of misuse by other Students, they should talk to a teacher about it as soon as possible.

- School Devices are owned by Haberdashers' Elstree Schools Limited, and the School reserves the right to examine or delete any files, including email, that may be held on its computer system or to monitor any Internet sites visited. The School reserves the right to vary the terms of this agreement/policy at any time and without prior notice. The School has the right to withdraw access to the Network, suspend Internet access or email access. Network access will be suspended until any policy discrepancy has been finalised. The decision of the School is final. The latest Agreement is always available for download from the School website or by contacting the School. It is important that Students review the Agreement regularly to ensure they are aware of any changes.

- Any misuse of technology by Students will be dealt with under the School's Behaviour Policy. Incidents involving the misuse of technology which are of a safeguarding nature will be dealt with in accordance with the School's Safeguarding Policy in conjunction with the School's Behaviour Policy. If a Student is worried about something that they

have seen on the internet, or on any electronic device, including on another person's electronic device, they must tell a teacher about it as soon as possible.

5.2 Access and Security

- Passwords protect the School's network and computer system. User logon details must not be shared with another person. Students are responsible for their logon credentials and for all activity undertaken using those credentials. Students must not be allowed any form of access using a staff user's account. Failure to do so could allow unauthorised access to sensitive or confidential information. If Students believe that someone knows their password, it must be changed immediately.

- Students should take all necessary steps to prevent unauthorised access to information held on ICT systems at the School. Extra care should be taken with data that is classified as personal or sensitive under the General Data Protection Act (GDPR).

- No devices or remote access sessions should be left unattended and unsecured when a Student is logged in. To prevent unauthorised access Students must either logout or password lock any device whenever these are unattended.

- Information contained on School Devices is especially vulnerable and special care should be exercised when you are offsite. All storage within a School Device is encrypted. Students must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which they are not authorised to access. If there is a problem with the password, speak to ICT.

- Access to the internet from the School's computers and network must be for educational purposes only. Students must 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.

- If access is needed to information or systems to which a Student does not have permission, speak to a teacher.

- 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 Students think or suspect that an attachment, or other downloadable material, might contain a virus, they must speak to a member of the ICT team before opening the attachment or downloading the material.

5.3 School Devices

- School Devices are strictly for learning and educational purposes only.

- All School Devices are maintained by the School and must not be tampered with. Hardware should not be modified in any way, and all preinstalled software, including those for anti-virus, filtering and monitoring should not be disabled or removed.

- It is the responsibility of the Student in charge of the device to ensure their laptop is brought into School whenever required for major upgrades and maintenance.

- Students must not download or install any alternative browsers, including Chrome, onto their devices unless given permission by ICT or a teacher.

- Students must not download or install any other computer program or app, unless allowed by ICT or a teacher.

- Students must not play computer games or use chat programs on any School Device unless allowed by the teacher.

5.4 Use of Personal Devices, BYOD or Wearable Technology

- We do not operate BYOD in our School. Students must not bring in another device for schoolwork or entertainment. All learning must be completed on a School Device. For devices used for specialised purposes, students should discuss the use with a teacher and ICT before using on school site.

- Students in Y11 and below should not connect a Personal Device to the School network. This includes connecting a mobile phone to the school WiFi network. Mobile phones are not to be used during the school day. The exception is 6th Form Students are allowed to connect their mobile phone to the school WiFi network, but they are only allowed to use their phone in permitted areas.

- If a Student wishes to connect a Personal Device to the School network, this will be dealt with on a case-by-case basis. Some Personal Devices may not have the capability to connect easily to School systems. The School is not under any obligation to modify its systems or otherwise assist Students in connecting to those systems. In order to access School systems, it may be necessary for the ICT Support team to install software applications on a Personal Device. If any such software is removed, access to the School systems will be disabled.

- It is always the responsibility of those bringing Personal Devices to School to keep them in a safe place, either on the person or locked away. **The School does not accept any responsibility for replacing lost, stolen, or damaged Personal Devices brought onto School premises, including devices that have been confiscated of which have been handed in to staff.** Many devices have a location finder app and it is recommended that this feature is enabled to aid tracking wherever possible. It is also recommended that such devices are fully insured to cover loss and damage outside of the home.

- Students are not permitted to wear or use smartwatches or any connected wearable device during the school day.

- Fitness trackers without messaging, calling, or voice assistant functions may be worn, but must not become a source of distraction.

- Wearable cameras, microphones, or audio recording devices are strictly prohibited at all times, except where explicitly approved as a reasonable adjustment for a disability.

- Smart glasses are not permitted, including those with prescription lenses. Prescription functionality does not override the safeguarding and privacy concerns linked to their recording or connectivity features.

- School-owned VR headsets may be used in the Innovation Centre, under direct staff supervision, as part of structured and approved learning activities. These must not be used outside of this context.

- All Wearable Technology and Personal Devices must be removed and handed in before the start of any examination or formal assessment, or any assessment at the teacher's discretion. Possession of a smartwatch or other connected wearable device during an examination is considered malpractice and will be treated accordingly, in line with JCQ regulations. It should be noted that all watches, including analogue watches, are not permitted by JCQ. Students found in possession of a mobile phone or Personal Device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

5.5 Internet, Email and Communications

All Students will receive guidance on the use of the School's internet and email systems. If a Student is unsure about whether they are doing the right thing, they must seek assistance from a member of staff.

For the protection of all Students, their use of email and of the internet will be monitored by the School. Students should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Students should not assume that any files stored are private.

Students using Personal Devices are expected to use them in accordance with this policy and by using any such device in School, Students agree to be bound by the additional School rules and requirements set out in this policy.

- Students must take care to protect personal and confidential information about themselves and others when using the internet. Students should not put personal information about themselves, for example their full name, address, date of birth, mobile number, or information identifying the school they attend online.

- Students should 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. Students must not copy (plagiarise) another's work.

- Students must use their school email accounts for all email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

- Email should be treated in the same way as any other form of written communication. Students should not include or ask to receive anything in an email which is not appropriate to be published generally or which they believe the School and / or their Parents would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone they did not intend.

- Students should carefully consider security prior to sending emails and communications which contain personal data or passwords.

- Students must exercise caution when opening e-mail attachments, as these may contain viruses. Unsolicited emails, emails from an unknown source or emails from a known source that seem "out of character" should be treated with extreme caution. If in doubt, deletion, without opening the email, is the safest course of action. ICT Support is available to give advice if needed.

- Students must not read anyone else's emails without their consent.

- Students should be aware that many social media sites have a minimum age of 13 years old.

- Anything posted online whether through messaging, social media or by other means needs to be considered carefully. Remember that there is a 'disinhibition effect' making a Student more likely to post things they might regret. The School may become involved in anything between members of the School community or that may bring the School into disrepute.

- Private conversations are rarely private and should not be considered so.

- Only messages or images that a Student would be happy for a teacher, Parent, or guardian to see should be posted. Avoid making strongly opinionated comments which could be deemed offensive. Avoid making comments related to protected characteristics.

  Anonymous posting is unwise. If Students set up accounts to post anonymously (or that the presence of a group allows anonymity) all members of the group will be deemed individually responsible for material posted unless an individual admits responsibility. Nevertheless, other members of the group will be deemed partially responsible unless they have reported inappropriate posts or actively attempted to dissuade the perpetrator.

- Some messages and images may seem to be temporary and permanently deleted – this may not be the case if screenshots or photos are taken. Treat all posts as permanent.

- Be careful not to believe all that is read online. Some sites publish dangerously inaccurate material. Be especially careful when investigating health concerns, sexuality and identity and searching for supportive communities.

6 Prohibited Activities

All Students will receive guidance on the use of the School's internet and email systems. If a Student is unsure about whether they are doing the right thing, they must seek assistance from a member of staff.

For the protection of all Students, their use of email and of the internet will be monitored by the School. Students should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Students should not assume that files stored on servers or storage media are always private.

Students are expected to use Personal Devices in accordance with this policy and by using any such device in School, Students agree to be bound by the additional School rules and requirements set out in this policy.

7 Monitoring and Privacy

All records created in accordance with this policy are managed in accordance with the law and the School's policies that apply to the retention and destruction of records.

The records created in accordance with this policy may contain personal data. The School has Privacy Notices which explain how the School will use personal data about Students and parents. The Privacy Notices are published on the School's website. In addition, staff must ensure that they follow the School's Data Protection Policy when handling personal data created in connection with this policy. Information Security and Sharing Data guidance is also contained in the Data Protection Policy.

The School has a firewall in place to ensure the safety and security of the School's network. Students must not attempt to disable, defeat or circumvent any of the School's security facilities.

The School has web filtering and monitoring systems in place to block access to unsuitable material, harmful content wherever possible, to protect the welfare and safety of Students. Students must not try to bypass this system.

All School Devices have monitoring systems installed, and students must not attempt to block or circumvent these. The monitoring system is used in accordance with KCSIE guidelines and exists for the safety of all Students.

Please note the following in terms of when we will be monitoring:

- Any alerts that come through outside of school hours during term time will not be picked up until the following working school day.
- We will not be picking up or reviewing any alerts that come through outside of term time.
- Alerts only come through from activity on school-owned devices and not personal devices.

Teachers have access to classroom monitoring tools and can view a School Device screen at any time during the school day. This also includes if a School Device is off site (e.g. a student is ill at home). Teachers have been advised to use classroom monitoring tools during lessons at their own discretion. They can monitor devices their own lessons or cover lessons, and is used to ensure Students are on task, rather than for continuous surveillance. Heads of House, Heads of Sections and DSLs may view any Student Device screen at any time during the school day if there is a safeguarding concern or suspicion of device misuse.

8 Sanctions and Disciplinary Actions

Where a Student breaches any of the School's rules, practices or procedures set out in this policy or the appendices, the respective Head, or delegated staff member, will apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Behaviour Policy including, in the most serious cases, permanent exclusion.

Unacceptable use of technology could lead to the confiscation of a Personal Device or deletion of the material in accordance with the procedures in this policy.

If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence e.g. upskirting, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police.

The School reserves the right to charge a Student or their parents for any costs incurred to the School because of a breach of this policy.

For information concerning confiscation/liability please refer to: https://assets.publishing.service.gov.uk/media/62d1643e8fa8f50bfbefa55c/Searching__Screening_and_Confiscation_guidance_July_2022.pdf

For less serious offences, typically a Student can expect a Lunchtime Detention / L1, or an After School Detention / L2:

- Personal Devices confiscated can be picked up from the designated area at the end of the school day. The student can expect a Lunchtime Detention / L1. For persistent offences, these will be dealt on a case-by-case basis with the DSL or a member of the Senior Leadership Team, but devices may be kept for more than 24 hours and a more severe sanction.

- Students playing games during a lesson can expect an After School Detention / L2. Outside of lessons, but while on the school site, sanctions are at the discretion of the supervising teacher. For persistent offences, these will be held in discussion with the student by the Pastoral team, but the student may expect limited device usage and increased monitoring.

All other cases will be dealt on a case-by-case basis between the Student and a member of staff.

9 Sanctions

Where a Student breaches any of the School's rules, practices or procedures set out in this policy or the appendices, the respective Head will apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Behaviour Policy including, in the most serious cases, permanent exclusion.

Unacceptable use of technology could lead to the confiscation of a device or deletion of the material in accordance with the procedures in this policy.

If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence e.g. upskirting, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 4 for more information on photographs and images.

The School reserves the right to charge a Student or their parents for any costs incurred to the School because of a breach of this policy.

10 Student Agreement

I understand that use of the ICT resources at Haberdashers' Elstree Schools Limited, which includes The Haberdashers' Boys' School and Haberdashers' Girls' School must be in support of educational research or learning and must not in any way bring the School's name into disrepute. I agree to the following:

- I will only log in to any School Device using my own username and password. I will keep my password secure and not share it with anyone.
- I will notify a member of staff immediately if I identify a security problem including spam or viruses.
- I will refrain from accessing any internet site that would be considered as offensive by the School or my parents/guardians.
- I will not use School Devices to play non-educational games or access social media/messaging platforms. I will not download materials that may be copyrighted nor will I violate copyright laws.
- I will not use, send or receive any material that could cause offence or harassment or is illegal. I will be courteous and use appropriate language in any email I send to other users. I understand that the laws of libel and copyright may apply to email.
- I will not misuse generative AI, particularly in the creation or distribution of harmful content, such as deepfakes or discriminatory material. I will not upload photos of any student or staff member into GenAI platforms.
- I will not include any defamatory remarks about the School in any electronic communication including postings to any websites, social media platforms or online streaming services.
- Plagiarism is unacceptable. I will use downloaded materials in an appropriate manner in assignments, listing them in a bibliography and clearly specifying directly quoted material. Failure to disclose sources may lead to exclusion from public exams.
- I will not reveal any personal information of any type about others or myself.
- I understand that the School web filter monitors all Internet activity and I will not try to bypass the filtering and monitoring system in any way.
- I will use my OneDrive, Teams or shared resource areas for the purpose of education only – I will not store any data or programs which are not part of my curriculum.
- I will not store any files other than School-related work.
- I will not interfere with the set-up of software or hardware of any kind on any School Device. If there is a problem with the School Device, I will not attempt to fix it myself but will inform the appropriate member of staff.
- I will not exploit the use of any mass media communication technologies for instant messaging, file sharing, audio/video conferencing e.g. Skype, MS Teams, Zoom, etc. and understand it is a means of communication for Students and their families only.
- I am aware of my social responsibilities regarding using the internet and related technologies, including treating others with respect and reporting instances of online bullying.
- I understand that there may be occasions when I will access the internet without direct staff supervision and I agree to abide by the above.
- I must not use the School email account for engaging in any form of commerce.