Habs

HABERDASHERS'
ELSTREE SCHOOLS

Acceptable Use Policy – Students

Please read this document carefully and discuss with your child

Policy Type	Non - Regulatory
Last Review	Summer 2023
Next Review	Summer 2024

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 peer-to-peer 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

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

E-Safety Policy
Safeguarding Policy
Anti-Bullying Policy
Behaviour Policy
Data Protection Policy
Privacy Notices

3 Terminology

BYOD means Bring Your Own Device, enabling Students to use their own devices in School.

Personal Devices include laptops, mobile phones, smart watches, tablets, iPods, MP3 players, and games consoles.

Head, where not explicitly defined, means the Head of the Boys' School or the Head of the Girls' School.

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

School means Haberdashers' Aske's Elstree Schools Limited as Trustee of Haberdashers' Aske's Charity trading as Haberdashers' Girls' School **and/or** Haberdashers' Boys' School, as now or in the future constituted (and any successor).

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 (such as firefly)
- SMART boards; and
- other photographic or electronic equipment e.g., GoPro devices.

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.

5 Safe use of technology

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.

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

Any Student who has been allowed to use Personal Devices in School is not permitted to use them in specific areas such as changing rooms, toilets and swimming pools.

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

6 Internet and email

All Students will receive guidance on the use of the School's internet and, where accessible, 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.

7 Using School Systems and BYOD

The Schools recognise the benefits to learning from offering Students the opportunity to use Personal Devices in School and is committed to help Students access these in the most efficient way to support their learning. It is the intention of this policy to facilitate and support the use of Personal Devices in School in furtherance of individualised Student learning. 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.

8 School Rules

Students **must** comply with the following rules and principles:

- Access and security (Appendix 1)
- Use of internet, email and online communication (Appendix 2)
- Use of Personal Devices or BYOD (Appendix 3)
- Photographs and images (including "sexting") (Appendix 4)

The purpose of these rules is to set out the principles which Students must always bear in mind and the rules which Students must follow to use technology safely and securely.

These principles and rules apply to all use of technology.

9 Procedures

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.

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.

Students must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Bullying Policy. If a Student thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher about it as soon as possible. See the School's Anti-Bullying Policy for further information about cyberbullying and e-safety, including useful resources.

In a case where the Student is potentially vulnerable to radicalisation, they may be referred to the Channel programme in accordance with the School's Safeguarding Policy. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into extremism (including terrorism).

10 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.

11 Record keeping

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 computer system is owned by Haberdashers' Aske's 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.

Appendix 1
Access and Security

General

- 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 securely lock any device whenever these are unattended.

- Information contained on School devices is especially vulnerable and special care should be exercised when taking these offsite. All storage within a School device is encrypted.

- Copyright of all material must be respected.

- 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.

- 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 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 a teacher.

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

- All School-owned laptop computers and mobile devices must be maintained by the School only. Anti-virus and software updates will be managed automatically although it is the responsibility of the Student in charge of the computer to ensure their laptop is brought into School whenever required for major upgrades and maintenance.

- 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.

- 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 IT team before opening the attachment or downloading the material.

- Students must not disable or uninstall any anti-virus software on the School's computers.

- The use of location services represents a risk to the personal safety of Students and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while on School premises or otherwise in the care of the School is discouraged.

- Students must NOT download or install any alternative browsers, including Chrome, onto their devices.

Personal Devices

- Use of any Student laptop or other device connected to the School's Wi-Fi is also covered by this policy regarding acceptable behaviour. Students should not access internet using 3G/4G or other mobile internet connections independently of the school Wi-Fi whilst on School premises or otherwise in the care of the School do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour. If a Student's device can access the internet outside of the School's Wi-Fi network, then parents should also ensure that appropriate security and filtering is enabled on their child's device.

- Some Personal Devices may not have the capability to connect 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 IT Support team to install software applications on a Personal Device. If any such software is removed, access to the School systems will be disabled.

Appendix 2

Use of the internet, email and online communication

General

- The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

Use of the Internet

- 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 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, any form of bullying, pornographic, defamatory, or criminal activity. Using technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Students must tell a member of staff immediately if they have accidentally read, downloaded or been sent any offensive material or material that is inappropriate, including personal information about someone else.

- Students must not communicate with staff using social networking sites or other internet or web-based communication channels.

- Students must not bring the School into disrepute through their use of the internet.

Use of Email

- 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, and attachments should be password protected, and send the password to the recipient using an alternative method, e.g. a phone call or SMS.
- 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. IT Support is available to give advice if needed.

- Students must not send any email message which contains offensive material.

- Trivial messages and jokes should not be sent or forwarded through the School's email system. 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.

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

Other online communication (including social media, Zoom (chats) and Microsoft Teams)

- Where inappropriate usage of communications is identified, this may lead to disciplinary action being taken against the Students including suspension, and/or legal action.

- 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.

- Never pose as anyone else or any organisation.

- Do not make comments about individuals or the School online. These views could cause offence and the internet is not the place for such comments.

- 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.

Appendix 3
Use of Personal Devices or BYOD

General

- Personal Devices include but are not limited to mobile phones, smartphones, tablets and laptops.

- It is always the responsibility of those bringing mobile phones to School to keep them in a safe place, either on the person or locked away. **The Schools does not accept any responsibility for replacing lost, stolen or damaged mobile phones 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 where ever possible. It is also recommended that such devices are fully insured to cover loss and damage outside of the home.

- The Schools reserves the right to search the content of any mobile device – whether issued by the School or a Personal Device - where they have reasonable grounds for suspecting that the Student may have pornographic images or images likely to cause personal injury to any person (including the Student), or any other content prohibited in this policy.

- Mobile devices – whether issued by the School or Personal Device - must not be used to:

    - Record, take or share images, video and audio at School (unless using devices for educational purposes);
    - Store and/access inappropriate/undesirable imagery or material, including those which promote pornography, violence or bullying of any description or which may be offensive, derogatory or otherwise contravene School policies
    - Bully, harass, intimidate, send abusive/inappropriate messages or attempt to radicalise others will not be tolerated, may amount to a criminal offence and will constitute a serious breach of discipline, whether or not in the care of the School at the time of such use.
    - Record, take or share any images, video and audio of other Students or staff at School.

Student Use of Personal Devices and Mobile phones

- This policy covers all Students on roll at the School including visiting students. In particular, this policy applies to Sixth Form Students, and any other Student(s) who have been allowed in exceptional cases, to bring their own Personal Device including any accompanying software or hardware (referred to as a device in this policy), for learning purposes.

- Students may use mobile phones in a constructive context in classrooms as educational tools, **providing the express permission of the individual member of staff has been obtained beforehand**. Generally, mobile phones should be out of sight unless directed by the teacher.

- Mobile Phone users are advised that taking photographs or video of staff without their permission is against School rules and likely to result in significant sanctions. The

School recognises that mobile phone features are so commonplace to teenagers that they are likely to use mobile phones to photograph or video their peers without considering the need for consent – ideally consent would be sought beforehand but of greater importance is what use is made of photos and videos. Inappropriate use, e.g. posting on social media without consent, bringing the School into disrepute or defamation of character, is likely to lead to sanctions especially if the actions could be considered as harassment or bullying. **The sending of, or recording of unwanted, offensive, or threatening messages or images is illegal and such information may be forwarded to the police.**

- Mobile phones and Personal Devices must not be taken into examinations. 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.

- If there is suspicion that material on a Student's Personal Device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

- Failure to adhere to these regulations may result in confiscation, a ban and/or a punishment. Confiscated phones will be returned at the end of the School day for the first offence but may be kept for 24 hours or longer for subsequent offences at the discretion of the DSL or a member of the Senior Leadership Team.

For information concerning confiscation/liability please refer to:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf

Appendix 4
Photographs and Images

Photographs and Images

- Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

- Students may only use cameras or any mobile 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.

- Students must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so. If the material found is a pornographic image of a child or an extreme pornographic image this will not be deleted, and the device will be delivered to the police.

- If material found on a device is a still or moving image that has been obtained by 'upskirting' this will not be deleted and the device will be delivered to the police.

- The posting of images which in the reasonable opinion of the School are offensive or which brings the School into disrepute on any form of social media or websites, such as YouTube, is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

Sharing of Nudes or semi-nudes (also called Youth Produced Sexual Imagery)

- This refers to the taking and sending or posting of images or videos of a sexual or indecent nature of themselves or another Student, usually through mobile picture messages or webcams over the internet.

- The sharing of nudes or semi-nudes may be a criminal offence, even if the picture is taken and shared with the permission of the person in the image.

- Remember that once a photo or message is sent, the Student does not have control about how it is passed on. An image may be deleted, but it could have been saved or copied, and may be shared by others.

- 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.

- Should a student report that they have sent or received images, the School will treat incidences of youth-produced sexual imagery as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding Policy). If a Student is concerned about any image they have received, sent, forwarded, or otherwise seen, speak to any member of staff for advice and we will do all we can to support such as trying to get the images removed through the Internet Watch Foundation.

Upskirting

- Upskirting typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing parts of their body or clothing, not otherwise visible, to obtain sexual gratification, or cause the victim humiliation, distress, or alarm.

- Upskirting is strictly prohibited, whether a Student is in the care of the School at the time the image is recorded, or not.

- Upskirting is a criminal offence. Attempting to commit an act of upskirting may also be a criminal offence e.g. if actions are taken to do something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a telephone or camera but failing to do so because of lack of storage space or battery.

- The School will treat incidences of upskirting as a breach of discipline and as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding Policy).

- If a Student is concerned they have been a victim of upskirting, they should speak to any member of staff for advice.

ICT Acceptable Use Agreement for Students

I understand that use of the ICT resources at Haberdashers' Aske's Elstree Schools Limited, which includes The Haberdashers' Aske's Boys' School and Haberdashers' Aske's School for Girls 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 keep my password secure and will only use a network computer whilst logged on with my correct username and password.
- I will not share my username and password with anyone. I will always log off when leaving a workstation even for a short period.
- I will notify a member of staff immediately if I identify a security problem including spam or viruses.
- I will refrain from accessing any newsgroups, links, list-servers, Web Pages or other areas of cyberspace that would be considered as offensive by the School or my parents/guardians, because of pornographic, racist, violent, illegal, illicit, immoral or other content. I am responsible for rejecting these links if any appear inadvertently during my research. If such a website appears, I will report it to a member of staff.
- I will not use school devices or networks to play non-educational games or access social media/messaging platforms. I will not download materials that may be copyrighted. I will not 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 include any defamatory remarks about the School in any electronic communication including postings to any websites, social media platforms (e.g. Snapchat, Instagram or TikTok) or online streaming services (e.g. YouTube).
- 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.
- 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; this includes all multimedia files i.e. videos and music.
- I will not interfere with the set-up of software or hardware of any kind. If there is a problem with a system.
- If there is a problem with the School system, 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/cyber bullying.
- I understand that there may be occasions when I will access the internet without direct staff supervision e.g. when using computers out of hours or using the School's internet hotspots, but I agree to abide by the above.
- I must not use the School email account for engaging in any form of commerce.