Habs

HABERDASHERS'
ELSTREE SCHOOLS

Acceptable Use Policy – Staff

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

1 Background

Haberdashers' Aske's Elstree Schools Limited, which includes The 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.

The aims of this policy are as follows:

- to encourage active participation and support of every member of staff, Student, and visitors who deal with information and/or information systems;
- to safeguard and promote the welfare of staff, Students and visitors 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 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
Data Protection Policy
Staff Privacy Notices

3 Terminology

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

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

the School means Haberdashers' Aske's Elstree Schools Limited as Trustee of Haberdashers' Aske's Charity trading as Haberdashers' Boys' School and/or Haberdashers' Girls 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
- 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.

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

4 General Use and Ownership

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

Users are responsible for exercising good judgment regarding the reasonableness of personal use. For Staff, individual department heads are responsible for addressing issues concerning the personal use of the School's IT systems.

5 Security and Proprietary Information

- Staff 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).

- User logon details must not be shared with another person. You are responsible for your logon credentials and for all activity undertaken using those credentials. In particular, 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.

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

- Information contained on laptop computers and other mobile devices is especially vulnerable and special care should be exercised when taking these offsite. All storage within a laptop computer or mobile device must be encrypted.

- 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 user in charge of the computer to ensure their laptop is brought into School whenever required for major upgrades and maintenance.
- Copyright of all material must be respected.

6 Access and security

- If you need to access information or systems to which you do not have permission, you need to speak to your line manager.
- The School has a firewall in place to ensure the safety and security of the School's network. You 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 Staff and Students. You must not try to bypass this system.
- You must not disable or uninstall any anti-virus software on the School's computers.

7 Use of email

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

- Staff sending material which is CONFIDENTIAL should consider whether email is the most appropriate medium for communicating this information. Staff 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.

- Staff should seek to limit the amount of personal data contained in communications and if sensitive personal data is involved (this includes information about an identifiable individual's race or ethnic origin, religions, or similar beliefs, physical or mental health conditions, sexual orientation/behaviour).

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

- Staff must only use their school email accounts when contacting Students, Parents, or any other member of staff for any school related business.

- Users 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.

- You must not send any email message which contains 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. If you are unsure about the content of a message, you must inform your teacher in case you're a Student; or for Staff, please speak with your Line Manager. If you come across such material, you must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

- 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.

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

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

Anything you post online whether through messaging, social media or by other means needs to be considered carefully. Remember that there is a 'disinhibition effect' making you more likely to post things you 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 post messages or images you would be happy for a teacher, Parent or guardian to see.
- Avoid making strongly opinionated comments which could be deemed offensive. Avoid making comments related to protected characteristics.
- Anonymous posting is unwise.
- Do not make comments about individuals or the School online. They may be your views, but they could cause offence and the internet is not the place for such comments.
- Never pose as anyone else or any institution.
- 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.

9 Personal Devices (including Mobile Phones)

The Schools recognise that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and Parents/carers, but technologies need to be used safely and appropriately within Schools.

9.1 General Expectations

- Mobile phones and personal devices are not permitted to be used in specific areas within schools such as changing rooms, toilets and swimming pools.
- The Schools accept no responsibility for replacing lost, stolen or damaged mobile phones.

- The Schools reserves the right to search the content of any electronic 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.
- Electronic devices must not be used to
    - Record, take or share images, video and audio (unless using school 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 you are 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.

9.2 Student Use of Personal Devices and Mobile phones

- Mobile phones or personal devices will not be used by Students during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- 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.

9.3 Staff Use of Personal Devices and Mobile Phones

Staff are advised to:

a) ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
b) not use personal devices during teaching periods, unless written permission has been given by the head teacher, such as in emergency circumstances.
c) ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

- If a member of staff breaches this policy, action will be taken in line with the Schools' Employee Code of Conduct.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.
- Members of staff will have access to a work phone, where contact with Students or Parents/carers is required. All staff will be issued with a work email address.
- The Schools reserves the right to search the content of any electronic device on officially provided devices at any time as part of routine monitoring.

9.4 Visitors Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) are requested not to use their phones in areas where Students are present. Phones should be kept in bags, unless permission has been given e.g. contractors using phones for servicing.
- Personal devices must be used in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, safeguarding and image use.
- We will ensure appropriate signage and information is displayed and provided to inform Parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or head teacher of any breaches of this policy.