Online Safety Policy
(including Staff and Students' Computer Acceptable Use Agreements)

This Policy should be read in conjunction with other School policies (all available on the School's website), particularly Preventing Radicalisation & Extremism, Safeguarding (Child Protection), Positive Mental Health, Anti-Bullying, Staff Code of Conduct, Allegations of Abuse Against Staff, Whistleblowing, Behaviour, School Suspension and Exclusion, PSHCE, Relationships & Sex Education , Data Protection and Computer Acceptable Use (see appendix to this policy). It has been devised in accordance with the following legislation and national guidance: Keeping Children Safe in Education (KCSIE), DfE 2025 ; Working Together to Safeguard Children, DfE 2026 ; Relationships Education, Relationships and Sex Education (RSE) and Health Education (July 2025); Education For A Connected World (UK CIS); The Counter-Terrorism & Security Act 2015, 'Prevent Duty Guidance: for England & Wales', HM Government 2023; Information Sharing: Advice for practitioners, DfE 2024; UK Council for Internet Safety (UK CIS) Online safety in schools and colleges: 'Questions from the Governing Board', 'Sexting in schools and colleges'; 'Teaching online safety in school' (DfE, Jan 2023), Education for a Connected World Framework (UKCIS, 2020) and DfE guidance on Meeting digital and technology standards in schools and colleges (2023). National Cyber-Security updates are also a vital source of information and guidance, such as https://www.jcq.org.uk/dfe-and-national-cyber-security-centre-ransomware-update/.

1. Rationale

ICT is a vital part of teaching and learning and is a crucial tool for staff and students alike. It also has an integral role in the School's management information and administration systems and also applies to the other devices used in school by students and staff such as school laptops, iPads and Chromebooks. Access to the Internet is an essential tool for all staff and a privilege for students. Online safety can be defined as the safe and responsible use of technology. This includes the use of the Internet, and also other means of communication using electronic media (eg text messages, gaming devices, online platforms such as Instagram and TikTok, email etc).

Included in Online Safety is online safeguarding, and this is an area that is constantly evolving.

The two overriding purposes of this policy are:

- To enable the whole School community to stay as safe and risk free as possible
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce the possibility of harm to a student or liability to the School.

The Online Safety policy is also important in School in order to:

- ensure there is a clear and consistent approach responding to incidents
- ensure that every person responsible for students is aware of his/her responsibilities
- set boundaries of use of any School-owned ICT equipment, or personal IT equipment used at HBS, and to set the boundaries of services such as social networking (e.g. X).

2. Terminology and Scope

For clarity, the Online Safety Policy uses the following terms unless otherwise stated:

Users - refers to teaching and support staff, governors, students and any other person working in or on behalf of the School, including contractors who use any of the School's ICT equipment or facilities.

Parent – any adult with a legal responsibility for the student outside of School e.g. parent, guardian, carer.

School – includes any School business or activity conducted on or off the School site, e.g. visits, school trips etc.

Wider school community – students, all staff, members of the governing body, parents.

Online safety can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm, for example: making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images) and online bullying; and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

3. Policy Governance (Roles & Responsibilities)

The Head has overall responsibility for online safety within the School. The day-to-day management of this will be delegated to other members of staff as indicated below.

The **Head** will ensure that:

- Online safety training and information throughout the School is planned and up to date and appropriate to the recipient, i.e. students, staff, governors, parents
- The Designated Safeguarding Lead (DSL) and IT Manager have had appropriate training in order to undertake the day-to-day duties needed to ensure online safety
- All online safety incidents are dealt with promptly and appropriately.

The **Deputy Head** is responsible for ensuring that:

- Computing and online safety is delivered as part of the curriculum across all subjects where relevant.

The **DSL** will:

- Take lead responsibility for online safety and safeguarding
- Be the first point of contact for all online safety-related incidents
- Liaise with the IT Manager and/or Heads of Year/Key Stage to follow up any online safety issues
- Support Heads of Year/Key Stage and the Head of PSHCE in delivering online safety awareness material within the tutorial and/or assembly programme, and ensure it is embedded within the PSHCE Programme

- Keep up to date with the latest risks to children whilst using technology; be familiar with the latest research and available resources for School and home use
- Discuss with, and advise, the Head on relevant online safety matters
- Engage with parents and the School community on online safety matters at School and/or at home
- Respond to any online safety incidents and follow local safeguarding guidance
- Liaise with the local authority, ICT technical support and other agencies as required
- Liaise with the IT Manager to ensure any technical online safety measures in School (e.g. Internet filtering and monitoring software, and behaviour management software) are fit for purpose and that the School meets the filtering and monitoring standards published by the DfE.

The **IT Manager** is responsible for ensuring that:

- The ICT technical infrastructure is maintained; this will include as a minimum ensuring that:
  - Anti-virus protection is fit-for-purpose, up to date and applied to all capable devices
  - All operating systems/system updates are regularly monitored and devices updated as appropriate
  - Any online safety measures such as Internet filtering and monitoring are operating correctly and meet the filtering and monitoring standards published by the DfE
  - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the DSL
  - Passwords are required for all users
  - For security reasons, the IT System Administrator account is to be used only for the purposes of system administration rather than day-to-day tasks. Third parties (i.e. engineers, contractors) requiring this level of access shall be provided with a separate account with appropriate privileges unless administrator access is absolutely necessary. This account shall then be removed or disabled on completion of said task at the IT Manager's discretion
  - The primary server is properly functioning except during maintenance or rebooting, including school holiday periods
  - Any personal data or software is removed from the PC/laptop if the individual is not authorised to receive the data
  - Care is taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently
  - The requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

Teaching and support staff will ensure that:

- They read and understand online safety information within the Staff Handbook and attend Staff Training as required, and agree to the Computer, Network and Internet Acceptable Usage Policy for Staff (Appendix A). Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Staff Conduct Policy. (All new staff receive online safety training as part of their induction programme; online safety is included in the annual Safeguarding Training given to all staff and additional training is provided as required.)
- All actions must comply with the legislation, including the Data Protection Act 2018, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988

- Any online safety incident is reported to the DSL or, in their absence, to the Head. In exceptional circumstances, an online safety incident may be reported directly to the Chair of Governors.
- Suspected or actual breaches of information or ICT security must be reported to the IT Manager, who will report immediately to the Head.

For **students**, the use of ICT equipment and services in School is a privilege and not a right. Before they are permitted access, students will:

- At the start of their time at the School, read and make sure they understand the Computer, Network and Internet Acceptable Usage Policy for Students (Appendix B),
- Understand that any deviation or misuse of ICT equipment or services will be dealt with in accordance with the this Policy and the School's Behaviour Policy.

Online safety is embedded into the curriculum. In particular, students will be given the appropriate advice and guidance by staff as part of the curriculum in Computer Science and PSHCE. Similarly all students will be made aware of how they can report areas of concern whilst at School or outside of School. The online safety curriculum includes material about: online self-image and identity; online relationships; online bullying; online reputation; managing online information; privacy and security (and see further below).

Parents play the most important role in the development of their children; as such the School will use its best endeavours to keep parents up to date with new and emerging online safety risks, through information evenings, newsletters and/or information on the School's website and will involve parents in strategies to ensure that students are made aware of such risks and that students are empowered to manage online safety risks appropriately. Parents must also understand that the School needs to have rules in place to ensure that their child can be properly safeguarded. The Computer, Network and Internet Acceptable Usage Policy for Students (Appendix B) is sent out to parents before their children join the School and parents are required to confirm that they and their children have read, understood and agree to it.

4. Technology

The School uses a range of devices including PCs, Macs, laptops, iPads and Chromebooks. In order to safeguard students and also to prevent loss of personal data the School employs the following technology:

(i) Internet Filtering prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites. In determining what is "inappropriate", the School meets the filtering and monitoring standards published by the DfE and this will be reviewed in line with this Policy or in response to an incident, whichever is sooner. Internet filtering is currently provided to the school by LGFL.

(ii) Effective monitoring is in place to help protect students from potentially harmful and inappropriate activities. The IT Manager (in conjunction with the School's Internet provider) is responsible for ensuring that the technology for filtering and monitoring is appropriate. The DSL receives reports and alerts from the monitoring technology and these are followed up in accordance with the School's safeguarding procedures. Internet monitoring is currently provided to the school by LGFL, who ensure that any potential Safeguarding issues are brought to the attention of the DSL/Senior Deputy DSL for investigation.

(iii) Email Filtering – software that prevents any infected email being sent or received by the School. Infected is defined as an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

(iv) Passwords – all staff and students must access any device using their unique username and a password. All School devices that hold personal data (as defined by the Data Protection Act 201 8) will be password protected. No data is to leave the School on an unprotected device; all devices that are kept on School property and which may contain personal data are protected. Any breach (i.e. loss/theft of device such as laptop, USB drives, mark books, SIMS (School Information Management System) access from home) is to be brought to the attention of the Data Protection Officer (DPO) immediately, who will inform the IT Manager and the Head. The DPO/IT Manager will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. Please refer to the School's Data Protection and Privacy Policy for more detail.

(v) Anti-Virus – All School devices will have anti-virus software. The same anti-virus software is used throughout all School owned devices.

5. Teaching Online Safety in School

The school follows statutory guidance and current best practice in teaching online safety in many areas of the curriculum and in particular through PSHCE and Computer Science.

The Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance (July 2025) contains information on what schools should cover in their RSE and health education curriculum, including in relation to online safety. This includes:

1. Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
2. Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues.
3. The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online.
4. Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images.
5. That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves

has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime.

6. What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online.
7. About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them.
8. That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong.
9. That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice.
10. How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns.
11. That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect student s who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it.
12. How information and data is generated, collected, shared and used online.
13. That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising).
14. That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion.
15. That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk.

The DfE's 'Teaching Online Safety in School' (updated January 2023) offers helpful guidance about how students can be taught what positive, healthy and respectful online relationships look like. The guidance notes that it is important to communicate the potential harms in a safe and beneficial way, so that students remain respectfully cautious and not fearful.

The Guidance comments that when teaching about these safeguarding topics (and others), staff should be mindful that there may be a young person in the lesson who is or has been affected by these harms. During or after a lesson, a student may be prompted to disclose about something that may have taken place online.

The Guidance also says that it is good practice to consult the DSL when considering and planning any safeguarding related lessons or activities (including online) as they will be best placed to reflect and advise on any known safeguarding cases, and how to support any students who may be especially impacted by a lesson.

In accordance with the above guidance, the School aims for a whole school approach so that it is embedded in everything the school does including:

- Creating a culture that incorporates the principles of online safety across all elements of school life
- Proactively engaging staff, students and parents/carers
- Reviewing and maintaining the online safety principles
- Embedding the online safety principles
- Modelling the online safety principles consistently

6. Mobile phones and other BYODs (Bring Your Own Devices)

School use of mobile devices, including laptops and tablets is becoming more commonplace as a means of delivering teaching and learning. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of online safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

It is to be recognised that it is the enhanced functions of many handheld devices that will give the most cause for concern and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent or inappropriate images, exploitation and bullying.

Mobile phones and handheld devices can also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. There is also a growing concern regarding the impact of use or excessive use of mobile phones on adolescents, in particular in relation to their mental health.

It must also be understood that should handheld devices be misused, there may be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

For all these reasons, and informed by recent government guidance (see (updated in Feb 2026)), the School is a predominantly 'mobile free' school. This means that:

- Students are required to ensure any mobile phones remain switched off and in their school bags or lockers for the entirety of the school day, from when they enter the school building to when they leave.
- As an exception and a privilege, sixth form students are allowed to use their mobile phones in the 'loft'. Sixth formers who require their phones to access work while studying will use the workspaces in the 'loft' rather than the library.
- There may be individual and occasional exceptions to this, for example when a teacher permits students to access their phones as part of an approved and directed activity in the classroom, but this will be supervised.
- Students are permitted to bring their own laptops or tablets, in order to study in the library.
- Sixth form students are permitted to use their own laptops or tablets in lessons with the consent of the relevant subject teacher. Other students may be given individual consent to do this, for example if required as a reasonable adjustment for a special educational need.

Mobile or electronic devices (including watches with or without online access) are not allowed in examination rooms.

All students must ensure that files stored on their phones or other electronic devices do not contain violent, degrading or pornographic images. The transmission of some information is a criminal offence. Students who are found to be in breach of this rule can expect to have their device confiscated; it will be returned to their parents or passed to relevant external agencies.

7. Examining Electronic Devices

The Head, the Senior Team and any other member of staff authorised to do so by the Head (as set out in the Behaviour Policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- poses a risk to staff or student s, and/or
- is identified in the school rules as a banned item for which a search can be carried out, and/or
- is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Head or DSL
- Explain to the student why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the student's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Head / other member of the Senior Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or Senior Deputy DSL) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing sear and semi-nudes: advice for education settings working with children and young people.

Any searching of student s will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The School's Behaviour Policy (which contains further information on searching, screening and confiscation).

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the School complaints procedure.

8 . School's website

The Head takes overall responsibility to ensure that the website content is accurate and that it is compliant with statutory DfE requirements. On a day-to-day basis this is overseen by the member of staff with responsibility for the School's website/social media.

9 . Social Media

All staff are instructed to always keep professional and private communication separate.

School staff will ensure that in private use:

- No reference should be made in social media to students, parents/carers or School staff
- They are not online friends with any student
- They do not engage in online discussion on personal matters relating to members of the School community
- Personal opinions must not be attributed to the School and personal opinions must not compromise the professional role of the staff member, nor bring the School into disrepute
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Students:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum
- Students are required to follow our Acceptable Use Agreement (Appendix B).

Parents:

- Parents are reminded about social networking risks and protocols through our Acceptable Use Agreement and additional communications materials when required.

10 . Digital images and video

At HBS:

- Permission for use of digital photographs or video is obtained in accordance with the School's Data Protection Policy;
- The School blocks/filters access to social networking sites unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their online safety education programme as part of the PSHCE curriculum and also taught to consider how to publish for a wide range of audiences;
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. They are taught the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. They are taught the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Students are taught that everyone in the School community must be treated with courtesy, respect, kindness and good manners. Bullying, cyberbullying, harassment, child-on-child abuse (which includes sexual violence and harassment), abusive language, intolerance of cultural, religious, social or any other difference, any form of racism, or other such forms of unpleasantness are completely unacceptable and will not be tolerated in our community. This includes conduct in person, in School, in writing and any online communication, whether public

or private. This is clearly stated in the school's Behaviour Policy which is clear that students must adhere to the Code of Conduct online as well as in face-to-face or any other in person or written communication.

- Students must not communicate online in any way that will bring a member of the school community (past, present or future) into disrepute or that will bring the School itself into disrepute. This includes sending messages, posting photographs, videos or memes to an individual or a private group or on any kind of public platform. This is reiterated in the School Suspension and Exclusion Policy.

11 . Online Safety Incidents: breaches of information or ICT security

All suspected or actual breaches of information or ICT security, including detection of computer viruses, must be reported to the IT Manager, who will inform the Head, immediately.

Review & Update:

This policy will be reviewed annually. It was updated in May 2026 .

See Appendices below:

Appendix A: Computer, Network and Internet Acceptable Usage Policy for Staff

Appendix B: Computer, Network and Internet Acceptable Usage Policy for Students

Appendix C: Guidance on appropriate ways of working online, which is applicable when remote learning is taking place (eg during a pandemic) and at other times.

Appendix A

Computer, Network and Internet Acceptable Usage Policy for Staff

Please note that this forms part of the School's Online Safety policy, which can be found on the School's website and was last reviewed in May 2026

General Guidance and Key Principles

Each member of staff has a responsibility for helping to ensure that all members of the school community are kept as safe as possible when using technology. Staff must, therefore, understand that their own behaviour should set an example and must not do anything that could lead to the School suffering a loss of reputation.

Staff must ensure that they are sufficiently aware of the issues around online safety, including cyber bullying, to be able to make a judgement about whether any activity they are planning or participating in involves any risks. If they feel the need for further training or advice, or help with identifying any risks, they will raise this with the DSL , Data Protection Officer (DPO) and/or Head or IT Manager.

If a member of staff becomes aware of any safeguarding incident involving technology, they will report it using the normal safeguarding procedures, as set out in the School's Safeguarding Policy.

Staff must understand that the School IT systems are primarily intended for School-related use. Access to all computer resources is a privilege and that access requires responsibility and adherence to the School's values and this Acceptable Usage Policy. Staff should limit their personal use to appropriate times and purposes. Staff must not use either the School's or their own technology in ways that put the School's systems at risk, prevent other users from legitimately making use of them, or bring the School into disrepute.

This guidance relates to the use of school systems both in and outside of school and includes (but is not limited to) school computers and connected equipment, network devices and infrastructure, remote access systems, school e-mail systems, and any other system used for School related work.

If a member of staff breaches this Acceptable Usage Policy then penalties will be enforced to protect the school, students and computer systems. All computer usage and websites visited are logged and this information will be used if ever required.

Specific Guidance

Technology changes rapidly and it is not possible to document every use or expected behaviour. For that reason, it is essential that staff are able to apply the principles of the School's Online Safety policy to new situations. Within the key principles set out above, as a minimum, the School expects the following commitments:

Personal Use and Professional Reputation

Members of staff must not communicate with students except through official systems (such as School email) and, in particular, will not become their 'friends' on social networking sites such as Facebook or, connect with them via social media such as WhatsApp or Snapchat.

Members of staff must separate personal and educational use of social media tools (for example X). Staff must understand that, for their protection and that of others, the School may monitor and record staff use of IT systems.

Members of staff must only use School equipment to take photographs and videos of students.

Communication

Email is an important part of today's communications systems. Use of the installed systems/connections is for legitimate work related/education purposes only and is encouraged to improve the quality of work, operational matters, education and development.

Members of staff must take care when writing emails or other messages. Due to the sometimes more informal nature of email, texts etc., it is easy to forget that it is a permanent form of written communication and that material can be retrieved even when it is deleted from a computer or other device that has been used.

Members of staff must not open any attachments to emails, unless they are from a known/trusted person/organisation, due to the risk of the attachment containing viruses, other harmful programs or inappropriate content.

If material in an email or other message is thought to be offensive, harmful or defamatory members of staff must alert the DSL immediately.

Content

Members of staff must not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will they try to use any programs or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Members of staff must ensure that they check any online materials or websites that they intend to use with students in advance of the lesson to ensure that they are appropriate and accessible from School systems.

Members of staff must immediately report any unpleasant or inappropriate material or messages, anything that makes them feel uncomfortable when they see it on-line, or anything that they believe poses a risk to a member of the School community.

Where work is protected by copyright, members of staff must not try to download copies (including music and videos) unless they have the permission of the copyright owner, either directly or within the terms of a school licence.

Staff are aware that monitoring software is in place on all school devices to which students have access; alerts and reports related to potentially inappropriate, illegal or harmful online activities on such devices are sent to the DSL and are followed up in accordance with the School's safeguarding procedures. All computer usage and websites visited are logged and this information will be used if ever required.

Data Protection

Staff must ensure that they do not leave a computer logged on after use or leave a computer logged

on unattended. They must not upload or send any personal information about staff or students unless satisfied that they are meeting the requirements of the Data Protection Act.

Security and Health & Safety

The security of software programs and data is most important. Staff must immediately report any damage or faults involving equipment or software, however this may have happened. All files/disks/storage devices must be virus checked by the IT Department. If a member of staff suspects that a virus is present on any piece of equipment they must report it immediately to the IT Department.

Staff must not install or attempt to install programs of any type on a machine, store programs on a computer, or alter computer settings. All software must be authorised by the IT Manager.

Staff must comply with Health & Safety Executive (HSE) guidelines on the use of VDUs, keyboards and work stations. They must take every reasonable measure to ensure that school equipment is not lost, stolen or damaged.

Artificial Intelligence (AI)

Artificial Intelligence (AI) tools are now widespread and easy to access. Staff may be familiar with generative chatbots such as ChatGPT and Google Gemini. The school recognizes that AI has many uses to help students learn, to help teachers teach and to cut workload. However, AI also poses a risk to sensitive and personal data and to the authenticity, accuracy and reliability of work. The use of AI in some circumstances also poses a safeguarding risk.

Staff are responsible for ensuring that any work they complete through AI meets the highest standards of accuracy and ethics and does not compromise the security or standards of the school.

To ensure that personal and sensitive data remains secure, no one is permitted to enter school-held personal data into unauthorized AI tools. If this were to happen, the data breach procedure set out in the school's data Protection and Privacy policy would be followed and the matter could be referred to the Staff Disciplinary Policy.

Staff should ensure they are complying fully with the school's Data Protection & Privacy Policy when handling school data electronically.

Agreement

By signing the Safeguarding/Handbook recipient list, staff confirm that they have read, understood and agree with the Computer, Network and Internet Acceptable Usage Policy for Staff. Breaching this policy will result in further action.

Appendix B

Computer, Network and Internet Acceptable Usage Policy for Students

Please note that this forms part of the School's Online Safety policy, which can be found on the School's website and was last reviewed in May 2026].

General Guidance

Students are responsible for good behaviour when using the school's computer resources, when communicating with other members of the School community and when communicating with those outside of the School community in a manner that could be seen to be representing the School. This relates to the use of school systems both in and outside of School and includes (but is not limited to) school computers and connected equipment, network devices and infrastructure, remote access systems, school e-mail systems, and any other system used for studies as directed by the supervising teacher.

The Internet is provided for students to conduct research in support of their studies. E-mail is provided to communicate with others, as determined by the supervising teacher. Access to all computer resources is a privilege and that access requires responsibility and adherence to the school's values and this Acceptable Usage Policy.

If a student breaches this Acceptable Usage Policy, then penalties will be enforced to protect the school, students and computer systems. This will be carried out in accordance with the School's Behaviour Policy which contains the expected code of conduct by students and possible consequences for infringements.

Monitoring software is in place on all school devices to which students have access; alerts and reports related to potentially inappropriate, illegal or harmful online activities on such devices are sent to the DSL and are followed up in accordance with the School's safeguarding procedures. All computer usage and websites visited are logged and this information will be used if ever required.

In addition, students are expected to behave online with courtesy, respect, kindness and good manners. Bullying, harassment, child-on-child abuse (which includes sexual violence and harassment), abusive language, intolerance of cultural, religious, social or any other difference, any form of racism, or other such forms of unpleasantness are completely unacceptable and will not be tolerated in our community. This includes whether students are using school IT equipment or their own and if they are doing so in school or out of school at any time.

Specific Guidance

Access and User Accounts

- Access must only be made via the user's authorised account name and password, which should not be revealed to any other person. If a student believes that security of their password has been compromised, they must inform a member of IT Support immediately.
- A student must not pose as someone else when asking to for account information or to change their password.
- A student must not trespass in another user's work folder or attempt to gain access to resources they are not authorised to see or make use of.

- Students must log out after every network session and not lock their workstations. Failure to log out could result in unsaved work being lost and/or another person accessing the account.
- Students must only store school-related files in their document folder.

Damage and Incorrect Use

- Damaging, or attempting to damage or hinder the correct operation of a computer or any other device is forbidden.
- The security of the computer systems must not be compromised.
- Uploading and downloading of software and installing or attempting to install a program of any type, is not permitted.
- Students are not allowed to store executables and system utilities in user areas or bring in/run these files from removable storage devices.
- Using the network to access, download, send or print inappropriate material such as pornographic, racist, sexist or offensive material (any type of non-educational related material) is strictly forbidden.

E-Mail

- Students are responsible for all e-mails they send and for contacts made which may result in an e-mail being received.
- When using e-mail to communicate with a student, member of staff or outside organisation from a school computer (if authorised by your supervising teacher) the school e-mail system must be used. The use of personal e-mail accounts in these situations is not allowed.
- Students should not communicate with members of staff on social networking sites such as Facebook or, connect with them via social media such as WhatsApp or Snapchat.
- It is the responsibility of the student to notify their supervising teacher or member of IT Support should they inadvertently open an e-mail containing inappropriate material or a computer virus.
- Using e-mail to harass, insult or attack others or to send offensive or inappropriate messages or pictures is strictly forbidden.
- Students are expected to adhere to the School's guidance on appropriate use of email which is set out in the School planners and communicated to students via the tutorial programme.

Internet

- All Internet activity must be for study purposes only unless otherwise authorised/supervised. Students are expected to respect the work and ownership rights of people outside the school as well as students and staff.
- Students must not intentionally visit sites that attempt to bypass the school filtering system.
- The use of chat rooms or any other instant messaging site or posting offensive messages in forums is strictly forbidden.
- It is the responsibility of the student to notify their supervising teacher or member of IT Support

should they inadvertently access a website containing inappropriate material or a computer virus.

- Playing games/quizzes is prohibited at all times unless authorised by the supervising teacher.
- Copyright laws must not be violated.
- Plagiarising – representing as one's own work, any materials obtained on the Internet, is not allowed. When Internet sources are used in students' work, the author, publisher and Web site must be identified. This includes the use of material generated wholly or in part through use of artificial intelligence.

Mobile and personally owned devices

- The School is a predominantly 'mobile free' school. Students are required to ensure any mobile phones remain switched off and in their school bags or lockers for the entirety of the school day, from when they enter the school building to when they leave.
- As an exception and a privilege, sixth form students are allowed to use their mobile phones in the 'loft'.
- There may be individual and occasional exceptions to this, for example when a teacher permits students to access their phones as part of an approved and directed activity with consent from a member of staff, but this will be supervised.
- Key Stage 5 students have been provided with managed and filtered Internet access for personally owned devices in the Main Building Library space to be used to aid their studies. However, Sixth formers who require their phones to access work while studying will use the workspaces in the 'loft' rather than the library.
- Students should not circulate photos or videos taken in the School buildings or on the School's premises which are identifiable as part of the School without the express consent of a member of staff.
- All students must ensure that files stored on their phones do not contain violent, degrading, pornographic or other inappropriate images. The transmission of some information is a criminal offence. Students who are found to be in breach of this rule can expect to have their phone confiscated; it will be returned to their parents and/or passed to relevant external agencies.
- Authorised staff are permitted to search a student and/or their possessions, confiscate such items and/or examine them (including data or files on an electronic device) in accordance with the School's Behaviour Policy and DfE guidance (see above).

Artificial Intellligence (AI)

Artificial Intellligence (AI) tools are now widespread and easy to access. Pupils may be familiar with generative chatbots such as ChatGPT and Google Gemini. The school recognizes that AI has many uses to help student students learn. However, AI also poses a risk to sensitive and personal data and to the authenticity, accuracy and reliability of student work and learning. The use of AI in some circumstances also poses a safeguarding risk.

Students are responsible for ensuring that any work they complete is their own, is as accurate as possible and is the result of their own learning. AI may be used for the completion of independent work where sanctioned or recommended by a teacher but a student must never pass off work

produced by someone else or by an AI source as their own work. This is classed as plagiarism.

Agreement

This Appendix is provided in advance of a child joining the School and the parent/guardian is required to confirm that they and their child have read, understood and agree with the Computer, Network and Internet Acceptable Usage Policy for Students. The parent/guardian and their child understand that breaching this policy will result in further action.

Appendix C

Guidance on appropriate ways of working online, which is applicable when remote learning is taking place, for example during a pandemic, and at other times.

Please note that this forms part of the School's Online Safety policy, which can be found on the School's website and was last reviewed in May 2026 .

It has been developed to assist in maintaining and appropriately adapting the School's online safeguarding roles and responsibilities for remote learning. It will also reflect any updated advice from Barnet Safeguarding Children Partnership and from the Local Authority in relation to online safety and Prevent duties. Details of the Prevent radicalisation and community safety guidance can be found at: https://www.barnet.gov.uk/community/community-safety/radicalisation-and-prevent Thebarnetscp.org.uk.

Key Online Safety and Prevent contacts

Role	Name	Contact details
Designated Safeguarding Lead (DSL) including Prevent Lead	Mrs Claire Leek	cleek@hbschool.org.uk
Data Protection Officer	Ms Joanna Avey	javey@hbschool.org.uk
Designated member of senior leadership team if DSL (and Deputies) cannot be on site	Mrs Denise Walker	dwalker @hbschool.org.uk
Link Governor for Child Protection, online safety, Prevent	Mrs Lisa Coffman	lcoffman@hbschool.org.uk

Note: Contact details for all other key safeguarding agencies are as referenced in our Safeguarding and Preventing Extremism and Radicalisation policies. This includes Barnet MASH, for students displaying concerning behaviour and Due Diligence and Counter Extremism Division of the DfE for concerns about staff.

Barnet Multi-agency Safeguarding Hub: 020 8359 4066; mash@barnet.gov.uk
DfE Counter Extremism Division: helpline (020 7340 7264) and report system (https://report-extremism.education.gov.uk/)
National Anti-Terrorist Hotline: 0800 789 321
Please use this Online Tool for Reporting Terrorist or Extremist Use of the Internet.

Reporting Harmful or upsetting content:

- reporting harmful online content to the UK Safer Internet Centre
- getting government advice and trusted resources from Educate Against Hate on safeguarding from radicalisation, building resilience to extremism, and promoting shared values

Personal data and our duty under GDPR

The School's Data Protection Policy remains in operation and can be found on the School's website. During a period of remote learning and working it is even more important that we consider how safely personal data is being shared. The School will ensure that:

- access to data systems is provided, to staff who need access, securely.
- staff will be careful when sharing personal data for access to online resources.
- contact details for themselves or others will be shared only when necessary to relevant staff/agencies.

Safeguarding

At times staff may be working remotely with students and this can be challenging. The overarching responsibly to safeguard students both in school and working online at home will remain paramount. This will include continuing to follow these important safeguarding principles:

- The best interests of children must always continue to come first
- If anyone has a safeguarding concern about any child, they must act on it immediately and report to the DSL
- Students should continue to be protected when they are online.
- Online advice and guidance will be shared with parents who are caring for children at home.
- Safe practice guidelines will be followed for virtual classrooms and videoconferencing.
- Ensure, wherever possible, students being educated at home are aware of the enhanced online risks eg risk of conspiracy theories, fake news and extremist groups.
- Promote and monitor good online behaviour
- Ensure that students have access to pastoral support
- Report all concerns to the DSL

Further advice and guidance on Prevent in Barnet can be obtained from:
Prevent Education Officer: liam.foote@barnet.gov.uk
Prevent Coordinator perryn.jasper@barnet.gov.uk or barnetcst@barnet.gov.uk

Bullying or abuse online

Any abusive behaviour will not be tolerated, this includes online bullying and any abusive, racist or derogatory comments made online. Also see the School's Safeguarding, Behaviour and Anti- Bullying Policies, available on the School's website.

Other sources of advice and information can be found as follows:

- advice on reporting online abuse from the National Crime Agency's Child Exploitation and Online Protection command
- advice and support from Anti-Bullying Alliance for children who are being bullied
- Schools can access the free Professionals Online Safety Helpline which supports the online safeguarding of both children and professionals. Call 0344 381 4772 or email helpline@saferinternet.org.uk. The helpline is open from Monday to Friday from 10am to 4pm.

All concerns should be reported following normal procedures.

Online safety in school

The School will continue to have appropriate filtering and monitoring systems in place in school. Where students are using computers in school, appropriate supervision will be in place.

Online safety when working remotely

Where staff are interacting with children online, they will continue to follow our existing Staff Code of Conduct and other relevant policies. All staff who interact with children, including online, will continue to look out for signs a child may be at risk. Any such concerns should be dealt with as the existing Safeguarding Policy directs. Where appropriate, referrals will be made to children's Multi-agency Safeguarding Hub and when required, the police, as usual. Online teaching will follow the same principles as set out in the staff Code of Conduct Policy and the Behaviour Policy. The School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- Where one to one communication is required, the student must have an appropriate adult present.
- Staff and students must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, avoid bedrooms wherever possible and use a neutral background (which should be blurred where the technology is available).
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use communication systems provided by the School to communicate with learners.
- Staff should record, the length, time, date and attendance of any sessions held.

IT staff will be available remotely to help resolve issues, where possible. If they are unavailable, then help can be sought from the School's supporting network company.

See the rest of this Online Safety and Acceptable Use Policy and other School policies including Safeguarding, Behaviour, Staff Code of Conduct, Prevent Policies, all available on the School's website. Other sources of advice:

- DfE advice on undertaking remote education safely
- UK Safer Internet Centre on remote education

Staff will continue to be alert to signs that a child may be at risk of harm online, and act on any concerns immediately, following our normal reporting and record keeping procedures. Students know that they, too, must report any concerns to a member of staff, and they will be signposted to other sources of support when required.

Staff working safely

Safe practice guidelines will be followed for virtual classrooms and videoconferencing. This includes:

- Always at least two students and/or two staff for online classrooms
- One-to-one must have a parent/responsible adult present
- Wearing appropriate clothing
- Ensuring the background to the presentation is appropriate
- The platform is approved i.e. Google Suite, email etc, and never use a personal account. Use of anything else must be approved by Senior Team.
- Report any breaches of data protection to the DPO (or as applicable)
- Document and report any calls to / from a parent etc.
- Report any cyber-attacks
- Report and document any incident in the teacher/a student's house that was seen by students, and any inappropriate behaviour of other adults online (e.g. in a student's house)
- Not share personal information
- Use School email accounts (not personal ones)
- Use School devices over personal devices wherever possible

Working with parents and carers

The School will make sure parents and carers:

- Are aware of the potential risks to children online and the importance of staying safe online.
- Know what the School is asking students to do online, including what sites they will be using and who they will be interacting with from School.
- Communicate within school hours as much as possible
- Communicate through the School channels approved by the Senior Team
- Know where else they can go for support to keep their children safe online.

This will be done by sharing information via parentmail and newsletters, following updates and advice received from places such as:
Safer Internet Centre
DfE advice and guidance
London Grid for Learning
ThinkUKnow
Educate against Hate
Parentzone
Childnet