HEATHSIDE SCHOOL
HAMPSTEAD

E-SAFETY POLICY

(INCLUDING ACCEPTABLE USE & USE OF OWN DEVICES)

Policy Author: Andy Mirza

Reviewed by: Nicholas Shaw, Head of Operations

Reviewed: April 2026

Next Review Date: April 2027

Introduction

The policy covers the safe use of all internet connected technology used at school, including technology used for electronic communication within the school and communication beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and any other network or internet connected device.

Managing access and security

The school provides managed internet access to its staff and pupils in order to enhance the education provided by the school and help pupils to learn how to assess and manage online risks, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

The school ensures that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is functioning and effective.

The school ensures that its equipment has adequate security and protection. Access to school networks is controlled by passwords and additional authentication. Different types of users have access to different parts of the school systems depending on their roles. As with all online systems, passwords should be unique, suitably complex and changed regularly.

Systems are in place to ensure that school internet use can be monitored and logged so if there are any incidents, the school can receive alerts and identify patterns of behaviour and inform e-safety policy.

E-Safety Lessons

The school incorporates periodic, age-appropriate e-safety lessons into the wider school curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

Pupils are also advised about current online risks, peer pressure, risky smartphone apps, websites, online games and social media trends. They are also advised never to share passwords, or give out personal details or information which may identify them or their location.

E-mail

Staff and older pupils may only use school provided email accounts for communication or access to the school systems. Staff to pupil or staff to parent email communication must only originate from a school email address. Any group emails sent to parents must be sent using the school's email groups provided for this purpose. Younger pupils are not given any access to the school email service.

Particularly confidential email containing safeguarding information for example, should use additional security such as 'Confidential Mode' provided by the school email system, to ensure it cannot be accessed by unauthorised recipients.

Any unexpected incoming email should be treated as suspicious and attachments not opened, or links clicked. Even if the author is known, any email attachments still may potentially be suspicious if its receipt was not expected or there are any doubts about the veracity of the email.

Emails containing links which prompt you to login to access should especially be treated with suspicion. If in any doubt contact the IT department for advice.

Publishing content

The contact details for published content e.g. the school website, or any other externally visible media will always be the school address, email and telephone number.

Permission will be obtained from parents or carers before photographs or names of pupils are published on the school website. Parents provide this consent on signed forms during the admissions process, and may be reaffirmed from time to time if circumstances change.

Any content which contains any excerpts or other content originating from a third party should always be checked for permission before being reused.

Data Storage

Any school data and files should only ever be stored and accessed via the school provided, cloud based systems. Local (offline) storage of any confidential data (e.g. containing names of pupils) on computers on laptops is only ever permitted temporarily on school owned equipment. If confidential attachments are inadvertently downloaded locally by opening attachments or generating reports, for example, they must always be deleted immediately after use.

Use of any other online or offline systems not sanctioned by the school to store any confidential data is totally prohibited.

Sharing confidential files or data externally must always be using approved methods and with the permission of the senior leadership team (SLT).

Software Usage

Generally all software used at school is cloud-based (accessed via the internet). There are a few exceptions which aren't totally cloud based that are used in the classroom, such as software designed for use with specific hardware, like for example interactive white boards.

Although we are always exploring new software products and services for use at school. Use of any software which is not currently licenced and approved by the school is not permitted. No software should ever be installed on a computer or app downloaded on school equipment without prior approval from the school.

Please do not start trials of new software services without prior approval from the management team.

Use of social media

The school does not permit staff and pupil access to external social networking sites whilst on the school premises, however it is sanctioned in certain circumstances in order to educate pupils in their safe use. This level of control may not mean blocking every site; it may instead involve monitoring and educating students in their use.

Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their position as a member of the school community.

The school admin team does use social media from time to time for marketing purposes.

Instant Messaging & Video Chat

Instant messaging services used to send instant text messages amongst groups of staff or pupils for any school related purpose or to coordinate any school related tasks may only be on platforms approved by the school.

Use of any external video chat and instant messaging services are not permitted on school premises by any staff, pupils or visitors unless it takes place using school approved platforms, using school accounts which are provided for the purpose.

Use of any other platform for specific purposes such as for communication with remote guests or speakers must be approved by the school on a case to case basis

Use of personal devices

Smart Phones.
While many students do carry smartphones whilst commuting to/from school, they are handed in for storage during the school day, and they are not permitted to be used by students whilst at school.

Teachers are permitted to use smartphones as authentication devices and are authorised to run a limited selection of school approved cloud-based apps. Using a smartphone on the school network results in a device management profile being automatically installed onto the device which allows the school to remotely remove any school data, if the smartphone is ever reported as lost or stolen.

This ability is provided for convenience and is not mandatory, and under no circumstances should smartphones be used to locally store any school data. To use a smartphone for extra features such as for a camera or for any potential local storage, you must only use a school owned smartphone or tablet. For general class photography, you are only permitted to use the school provided camera/tablet for your classroom, which can be booked out if necessary for school trips and events etc.

Other school owned smart devices (e.g. iPads) employ additional security restrictions and can be totally locked, wiped and have mandatory filtering of apps and sites.

Laptops.
Older school children are expected to use laptops regularly to access our homework portal, and older children, on occasion, do bring their laptops into school to assist in their day to day educational activities. We only recommend the use of Chromebooks by children, where the school can fully enrol them into our device management systems for safety and security. If it is not possible for a student to use a Chromebook, please contact our IT department, so we can assess if their device has adequate security to be used at school.

Staff using laptops at school, generally use school owned computers. However the school does recognise that some staff will prefer to use their own laptops, especially if they do not spend most of their time based at a single classroom or office, and often move between school buildings. You must inform us if you intend to use your own laptop so we can assess if it has adequate security to be used at school. Generally, higher-specced laptops are acceptable to use at school if they have encrypted storage by default.

Personal devices, laptops and computers may only be used by staff or pupils whilst on the school premises with the permission of the school. Staff and/or pupils may access the school IT systems remotely using their own devices, provided their use fully complies with this e-safety policy and the relevant Acceptable Use Policy (AUP).

Personal devices are not covered by school insurance policies or any warranties, and therefore, the school cannot be liable for any loss, theft or damage to personal devices. Using your own equipment is entirely at your own risk. However, if your device is ever lost or stolen, you must inform the school immediately.

Remote Learning

During exceptional circumstances such as periods of school closure, for instance during the COVID related lockdowns during 2020 and 2021, use of technology increased as the school switched to Remote Learning.

Remote access to school systems increases exponentially during a lockdown as all education is delivered online. This consists of having virtual classrooms where educational materials and links to resources are posted. Students can turn in work to be marked via the virtual classroom, and teachers can give individual grades and feedback.

While some lessons are recorded, most of the key curriculum is delivered via live video conferencing where students and teachers participate live.

Heathside's remote learning provision can be provided to all students. Whilst all students are expected to participate in a minimum number of daily hours of remote learning during lockdown periods depending on their age groups, we do ensure regular breaks away from screens are scheduled into their timetables. Please refer to our Remote Learning Statement for more information.

For pupils accessing our remote learning facilities, agreement of our e-safety and acceptable use policies is a primary condition of use. We recommend children only use remote learning on equipment approved by the school. The school only approves the use of Chromebooks by children, where the school can easily enforce additional security and protection measures. Use of any other type of computer or device provided by parents, requires children to be supervised by parents at home.

Authorising access on school premises

All staff (including volunteers) must read and sign the 'Staff AUP' before accessing any of the school IT systems or network.

For younger students, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials. For older students, access to the internet will be with teacher permission with increasing levels of autonomy.

Assessing risks and reporting

While the school will take all reasonable precautions to prevent access to any inappropriate or unsuitable material, due to the world-wide scale and ever-changing, linked internet content, it is not possible to guarantee 100% that any unsuitable material will never appear on a school computer or another device whilst on the school premises.

Any such incident must be reported to the Safeguarding Leads for further action, and followed up by the IT department to ensure the risk is blocked or mitigated. Furthermore, all Heathside Staff must contact their Safeguarding Leads if they suspect any student or staff member is using technology inappropriately, e.g. grooming, accessing age-inappropriate materials, or involved in possible radicalisation activities falling under our Prevent Duty. In all cases or if in any doubt, please contact the Designated Safeguarding Lead – See Safeguarding and Child Protection Policy.

Online Abuse

Staff and parents should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non- consensual sharing of images, especially around chat groups, and potentially the sharing of abusive images and pornography, to those who do not want to receive such content.

Handling e-safety complaints

Complaints of internet misuse by students will be dealt with according to the school's behaviour policy.

Complaints of a Safeguarding nature must be dealt with in accordance with the school's safeguarding and child protection procedures. In the first instance the Safeguarding Leads **must** always be contacted.

Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

Acceptable Use Policy

This e-Safety policy should be treated in conjunction with the Acceptable Use Policies (see appendices).

Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet. Pupils will be reminded about the contents of the AUP as part of their e-safety education. This especially applies to older pupils where students are expected to use the school's Virtual Learning Environment or Homework/Remote Learning Portals.

All school staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet at school.

Further Information and Resources

There is a wealth of information available to support schools and parents to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.pshe-association.org.uk
www.educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
https://www.ceop.police.uk/safety-centre/
http://www.cscb-new.co.uk/?page_id=95

Appendix A:

HEATHSIDE SCHOOL
HAMPSTEAD

Acceptable Use Agreement

(For All Staff, Volunteers and Guests)

New technologies have become integral to the lives of children and young people in today's society, both within the school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies whilst at school. All staff should consider this agreement to be an extension to the Code of Conduct.

This Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will endeavour to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible manner, to ensure that there is no risk to my safety or to the safety and security of the school systems and other users. I

recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care about the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, smartphones etc.) out of school, and to the potential transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. This includes any extremist material that may raise concerns under our PREVENT guidelines. If in any doubt, please contact your Safeguarding lead.

I will be professional in my communications and actions:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I will appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record images, unless I have explicit permission to do so. Where any images are published (e.g. on the school website or in the press) I will not identify by name (unless I have permission), or other personal information of those who are featured.
- I will only communicate with staff, students, and parents / carers using official school systems. Any such communication will always be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities. e.g. maligning the reputation of the school on social media with pupils, parents or staff.

The school has a responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date security software and are free from any malware.
- I will not use personal email addresses on the school systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any doubts or concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies. All school data should always be saved to the school provided Google Drive storage provided where backup is managed by the school.
- I will not try to upload, download or access any materials which are illegal (child abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or extremist (falling under the PREVENT guidelines) or otherwise inappropriate material which may cause harm or distress to others. I will immediately report any concerns accordingly. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless agreed by the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy. Where digital personal data is transferred outside the secure school environment, it must be encrypted using minimum SSL/HTTPS/HSTS technology. Paper based Protected and Restricted data must be held in secure lockable storage, and only ever transported using registered and safe methods. I understand that the data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and

confidential, except when it is deemed necessary that I am required by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies.

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the management team and / or the Local Authority and in the event of illegal activities, the involvement of other authorities.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: _____

Signed: _____

Date: _____

Appendix B:

HEATHSIDE SCHOOL
HAMPSTEAD

Acceptable Use Agreement

For Year 6 and above Students

Digital technologies have become integral to the lives of children and young people, both within and outside school. These technologies are powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and enhance awareness of context to promote effective learning. Young people have an entitlement to safe internet access.

The typical technology available to young people now can be used for a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, children need to learn skills to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of technology need to be harnessed to enhance children's learning.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal, and recreational use.

- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

I understand that I must use my school laptop and other school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that *Heathside School* may monitor my use of the systems, devices, and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will never communicate with strangers.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school-managed (including personal devices used for schoolwork) laptops and devices are primarily intended for educational use and that I will not use them for any other use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *Heathside School* systems or devices for online gaming, online gambling, internet shopping, file sharing, software piracy, or video broadcasting (eg YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (laptops, mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the *school.*
- I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand I will not try to upload, download or access any materials which may be illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. This includes access to any extremist material which falls under our PREVENT guidelines.
- If I observe anybody accessing any illegal, objectionable, or extremist material on any computer or device (whether owned by the school or not) I will immediately report it to our Safeguarding Team.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites whilst at school, unless this is for a usage directed by the school for a legitimate reason.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community

(examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the authorities.

Please sign the form on the next page to show that you have read, understood, and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

HEATHSIDE SCHOOL
HAMPSTEAD

Pupil Acceptable Use Agreement Form (to be countersigned by parents)

This form relates to the *student* Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use *Heathside School* systems and devices (both in and out of school)
- I use my own devices in *Heathside School* (when allowed) e.g. laptops, tablets, mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of *Heathside School* in a way that is related to me being a member of the school e.g., communicating with other members of the school, accessing school email, messaging systems, video chat, homework portal, website etc.

I understand:

- That all computer equipment I use for school work both inside and outside school will only be allowed access to school network and systems as long as I behave in a responsible way that keeps me and others safe.

- *I also understand that the school systems are monitored and that if I do not follow the rules, I may not be allowed access.*

I will:

- *I will only use computers and devices that connect to the school systems for school work and homework*
- *only delete my own files and not look at other people's files without their permission*

- *keep my login and password safe and not let anyone else use it or use other people's login or password*
- *not bring in files to school without permission*
- *ask a member of staff for permission before using the internet while at school*
- *not visit websites I know are banned by the school or use non-school email accounts or social networking sites*
- *only email people I know or whom my teacher has approved*
- *make sure any messages I send or information I upload is polite and sensible*
- *not open attachments or download files unless I have permission, or I know and trust the person who sent it*
- *not give out my home address, phone numbers or send photographs or videos or give any other personal information that may identify me, my family, or my friends unless my teacher has given permission*
- *never arrange to meet someone I have only met on-line unless my parent, carer or teacher has given me permission and I will take a responsible adult with me*
- *tell my teacher or responsible adult if I see anything I am unhappy with or receive a message I do not like, and I will not respond to any bullying messages*
- *only use my mobile phone or other device in school when I have permission*
- *not use any internet system to send anonymous or bullying messages or to forward chain letters*
- *log out when I have finished using the computer.*

Name of Student / Pupil: _____

Group / Class: _____

Signed: _____

Date: _____

Parent / Carer Countersignature

Signed: _____

Date: _____