Hayes School
(Part of the Impact Multi Academy Trust)

Policy Document

Policy Name	E-Safety Policy
Date of Last Review:	Summer 2025
Date of Next Review:	Summer 2027
SLT Responsible:	Assistant Headteacher

E-Safety Policy

Contents

1. INTRODUCTION

1.1 Policy Aims

Hayes School believes that the use of information and communication technologies in school brings great benefits. Recognising the e-safety issues and planning accordingly will help to ensure appropriate, effective and safe use of electronic communications.

This document also sets out the school's policy on social media and networking. New technologies are an integral part of our lives and are widespread powerful tools which bring new communication opportunities in teaching and learning for the school staff in many ways.

This policy together with the Anti-Bullying, IT User Policy, Child Protection and Safeguarding Policy, Staff Code of Conduct and Staff Discipline Policy is designed to keep staff and students safe in and out school when using ICT.

1.2 Writing and reviewing the E-safety policy

The E-Safety Policy relates to other policies including those for ICT, bullying, safeguarding and child protection. We will review this policy every year.

Hayes School's nominated E-Safety coordinator is Mr D. Loomes who will liaise with Hayes School's Designated Safeguarding Lead Officer, Mrs S. Arney over cases of e-safety concern.

1.3 The 4 categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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 scam

2. Teaching and Learning

2.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. Hayes School has a duty to provide students with high-quality internet access as part of their learning experience. Internet use will enhance and extend learning.

- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

2.2 Students will be taught how to evaluate internet content

- Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. This is evidenced in schemes of work in the ICT department.

- Hayes School internet access is designed expressly for student use and includes filtering appropriate to the age of students.

- Clear boundaries are set for the appropriate use of the internet and digital communications and are discussed with staff and students. Student education in e-safety takes the form of e-safety lessons in ICT and as part of the Personal Development curriculum (tutor time, ACTIVE and assemblies). Staff education takes the form of briefings and directing staff to the staff handbook for guidance. Parents are also informed of E-Safety at specific times throughout the year and through the newsletter.
- Students are educated through curriculum areas in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

- Online safety presentations take place every year for students with new students in Years 7 and 12 from an external provider. The same external provider also delivers an e-safety presentation which is made available to all parents and carers. The school informs and educates students on the following online safety issues and the actions they can take to protect themselves and report issues:

  (i) Inappropriate content: risks of being exposed to illegal, inappropriate or harmful material and methods for reporting such content;
  (ii) Contact: the risk of being subjected to harmful online interaction with other users.
  (iii) Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
  (iv) Commerce: risks such as online gambling, phishing and online scams
  (v) Accessing, sharing work and completing school work on-line
  (vi) Use and engagement with visual content particularly pictures and videos of themselves
  (vii) Live communications both verbal and visual

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

3. Managing Internet Access, e-mail and website content

3.1 Information system security

- Hayes School ICT system security is reviewed regularly. We use a range of products to protect the system. These include: Anti-Virus software, and a firewall on the servers. We also use a Proxy Server (Webscreen) that filters our internet traffic and allows IT services staff to track inappropriate internet usage by staff and students.

- The virus protection (Windows Defender and Sophos) is installed on all machines and servers. It downloads updates once a day at 7am and sends them to the client machines after it has been downloaded. Windows Defender scans the clients every Wednesday at 12.30pm.

3.2 E-mail

- All of the below is explicitly taught in ICT lessons and through ICT based assemblies.

- At present students are provided with a school based Outlook e-mail account, giving them an email and website access account. Students in Years 7-11 can only send internal emails to teachers and fellow students. Students in the sixth form are able to send emails to external addresses. Students may also additionally use Microsoft Teams platform to communicate and collaborate, but this is restricted to internal access and hosted through the school 365 platform.

- Students do not have system permissions to set up groups in Outlook for conversations.

- Students should immediately inform a member of staff if they receive offensive/inappropriate e-mail. Staff should inform their line manager.

- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- Staff and students should only open emails from people they know and attachments should not be opened unless the author is known. Regular checks and reminders are made on the validity of external content with the IT services team responding accordingly.

Staff additionally use Bromcom which supports a range of contact functions including e-mail and text messaging, and have received training on the safe and appropriate use of these functions in particularly the use of Bcc function in line with GDPR protection

3.3 Published content and Hayes School web site

- Staff email addresses are published on the school website. No student personal contact information will be published on Hayes School website. External email contact with Hayes School is made through limited source emails including the postmaster@hayes.bromley.sch.uk email account which is administered by the Principal's PA along with other school e-mail addresses registered to the domain @hayes.bromley.sch.uk (e.g. attendance@hayes.bromley.sch.uk)
- The Webmaster has overall editorial responsibility and ensures that published content is accurate and appropriate.

3.4 Publishing students' images and work [CI1]

Photographs that include students are selected carefully

- Students' full names are not used anywhere on a school web site in association with photographs.

- Permission to take or use photographs and images of students is obtained from parents via a consent form which is completed by parents when students join Hayes School. This information is recorded on Hayes School's management information system (Bromcom). The school webmaster needs to be aware of this and cross reference to any pictures on website.

  An additional checklist of students with photo permissions is included in all Education Visit packs to ensure trip leaders are able to manage and support the appropriate sharing of photographs taken outside of the school environment.

- Work can only be published with the permission of the student.

3.5 *Social networking, personal publishing and password security*
(see Appendix A for Social Media and Networking Guidelines for Hayes School Staff)

- Hayes School controls access to social networking sites, and considers how to educate students in their safe use.

- Newsgroups will be blocked unless a specific use is approved.

- Students are advised never to give out personal details of any kind which may identify them, their friends or their location.

- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future. Students should only invite known friends and deny access to others.

- Students are advised on user account security and how to set strong passwords (6 characters long, including a mix of upper and lower case & numbers).

- Students are advised to let their parents, carers, teachers, police or responsible adult know if they are uncomfortable about any contact made on social networking sites or over the internet.

- Parents are educated through after school e-safety talks on items such as parental locks and what to look out for whilst their children are on-line.

- Teachers should not become a "friend" of current students on social networking sites and should not communicate with students over the internet. Staff should only contact students using their school e-mail account, Bromcom, Microsoft Teams or via Satchel One for work purposes/school business in accordance with the Staff Code of Conduct.

- Students and staff should follow protocols for the use of Microsoft Teams, including for video interaction and only with students for whom parental consent has been obtained.

- Use of school Twitter accounts - e.g. setting up and use of school Twitter accounts to communicate with students such as the Drama Department Twitter feed must be approved by the Headteacher. Communications will be regularly monitored by the E-Safety co-ordinator.

4. Managing Filtering

- Hayes School works in partnership with Turn it On (TIO), our network provider and other schools, as appropriate to ensure that systems to protect students are reviewed and improved.

- If staff or students discover an unsuitable site, it must be reported to the classroom teacher who will inform the E-Safety Coordinator and/or IT Services who will block the site.

- IT services staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- E-Safety software has been installed across the school (Securus). This monitors all activity on the computers, across many categories including e-bullying, language, wellbeing, inappropriate content and activities.

- Monitoring of the Securus system is carried out daily by members of the Safeguarding team

5. Managing Videoconferencing

- All videoconferencing uses (Voice over Internet Protocol) VoIP with additional 'meeting room' areas being accessed through Microsoft Teams (staff and students) and Zoom (for staff use only)

- Students are not given access to VoIP. Teachers always lead VoIP sessions.

6. Managing Emerging Technologies

- Emerging technologies are examined for educational benefit and a risk assessment will be carried out before their use in school is allowed

- A mobile phone policy 'on site-out of sight' means phones should not be anywhere on the school site with the exception of 6th Form students who may use devices in designated 6th Form areas only. The sending of abusive or inappropriate text or other messaging is forbidden and should such messages be received students are encouraged to bring them to the attention of a member of staff so that appropriate action can be taken.

- The use of mobile phones by 6th Form students only may be permitted in lessons by a teacher to carry out research, use mobile applications or to photograph or film work under the close supervision of the teacher. Mobile phones should not under any circumstance be used to film/photograph students in lessons. Camcorders are available for this purpose from the Media Arts department.

- Staff members are to use Hayes School's phone system to contact students and not their mobile phones or in exceptional circumstances (e.g. COVID-19 School Closure) should ensure personal mobile numbers are withheld before contacting students, parents or carers.

- Staff should not use their personal phone camera/personal cameras to record student activity.

- The school recognises that many children have unlimited and unrestricted access to the internet via 4G and 5G [CI2]in particular and the school accordingly restricts the use of mobile phones on the school site. Parents/carers are advised by the school to ensure that appropriate filters are in place from their network provider.

6.1 Examining electronic devices

Members of staff with delegated authorisation from the Principal have the powers to search for prohibited items with the authorisation and presences of a senior member of staff in accordance with Department for Education Guidance on Searching, Screening and Confiscation as outlined in the Behaviour Policy

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 pupils and staff. If the search is not urgent, they will seek advice from Principal/DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

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 or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Undermine the safer environment of the school, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the DSL / Principal 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 if 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 pupil and/or the parent 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 equivalent) 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 nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils 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
- Our behaviour policy / searches and confiscation policy

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Hayes School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create

images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Hayes School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies. This includes any materials created to bully or harass staff.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 2018 (See the Data Protection Policy). The school is also fully compliant with GDPR laws.

8. Policy Decisions

8.1 Authorising Internet access

- By using a school 'log on' and signing onto the school domain either remotely or otherwise Hayes Staff accept/acknowledge they will comply with the protocols and conduct contained in the 'Staff ICT User Policy'.

- Hayes School maintains a current record of all staff and students who are granted access to school ICT systems.

- Students must comply with the Acceptable Use Policy in their learner handbooks and by logging on to the school network in school (or accessing their Office 365 account) are agreeing to this policy. This policy must be signed by both students and parents/carers at the beginning of each year.

- Students are allowed access to their user areas from home through OneDrive and SharePoint (Office 365). The same acceptable use policy applies at home as in school.

8.2 Assessing risks

- Hayes School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to Hayes School network. Hayes School cannot accept liability for any material accessed, or any consequences of Internet access.

- Hayes School audits ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective.

- In line with the Child Protection & Safeguarding Policy staff should not store images of students on laptops or personal devices.

8.3 Handling e-safety complaints

- Complaints of internet misuse will be dealt with in the first instance by the Network Manager who may refer it to a relevant senior member of staff.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Complaints of a bullying nature will be dealt with in accordance with both the child protection and safeguarding procedures, anti-bullying policy and behaviour management.

9. Communicating E-Safety

9.1 Introducing the E-Safety policy to students

- E-Safety rules are posted in all rooms where computers are used.
- Students will be informed that network and internet use is monitored.
- A programme of training in E-Safety has been developed, and is led by the ICT teaching team through lessons and assemblies supported by CEOP.
- The school website contains a link to e-safety resources.
- All students annually receive e-safety awareness training either internally or through an external provider.

9.2 Staff and the E-Safety policy

- All staff have access to the Hayes School E-Safety Policy, and its importance is explained.
- Staff are informed that their account and activities on the user account including the internet can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use clear procedures for reporting issues.
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- When staff are in email communication with parents/carer they should copy their line manager into any communications.
- Staff should not have images of students on mobile phones, staff personal cameras or on home computers.

9.3 Enlisting parents and carers support

- The attention of parents and carers will be drawn to Hayes School E-Safety Policy in newsletters and on the Hayes School website. This will include a list of e-safety resources, information and guidance for parents/carers from other organisations e.g. NSPCC, CEOP

- E-safety awareness training provided by Education Child Protection Limited is planned for parents annually. A parent's session took place in Autumn 2024. The slides from this session are available on the school website.

Parents can seek further guidance on keeping children safe online from the school website (E-Safety - Hayes School) and the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

CYBERBULLYING

Cyberbullying is:

– misuse of the internet to intimidate, including by e-mail and social media sites

- mobile threats by text message and call

- misuse of associated technology i.e. camera and video facilities

- sexting is when someone shares sexual, naked or semi-naked images of videos of themselves or others, or sends sexually explicit messages

Where any form of cyber bullying affects another pupil in the school or may bring the reputation of the school into disrepute, the school reserves the right to be involved whether the electronic material was produced within the school or outside. Furthermore, the school will review electronic material held or accessed by any pupil in the school including their e-mail account and their mobile phone if we suspect cyber bullying is occurring. Pupils must be aware that some forms and levels of cyber bulling are illegal and the school will inform the police where necessary.

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes ACTIVE lessons and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Links with other policies:

- Child protection and safeguarding policy
- Behaviour policy

10.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness with school leaders. The board will review the DfE filtering and monitoring standards, and discuss school leaders what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

10.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

10.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSLand deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

10.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

10.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix D), and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems and processes
- Following the correct procedures by contacting the DSL/Deputy DSL and ICT Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

10.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices D)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet

- Parent resource sheet – Childnet

10.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix D).

APPENDIX A. SOCIAL MEDIA AND NETWORKING GUIDELINES FOR HAYES SCHOOL STAFF

1. Introduction

(i) This document sets out the school's policy on social media and networking. New technologies are an integral part of our lives and are widespread powerful tools which bring new communication opportunities in teaching and learning for the school staff in many ways. It is important that we are able to use these technologies and services effectively but that this should be balanced with protecting our professional reputation and integrity. With this in mind, all staff working with students have a responsibility to maintain public confidence in their ability to safeguard their welfare, and to behave in the best interests of the students and the school. These guidelines are also designed to protect staff from possible harassment by a colleague or student via a social networking site.

(ii) These guidelines should be read in conjunction with the school's Child Protection and Safeguarding Policy, Staff Code of Conduct and Staff Discipline Policy. If staff fail to adhere to the guidelines set out, their conduct could be called into question and this may result in disciplinary action being taken against them which could ultimately lead to their dismissal.

(iii) Whilst these guidelines have attempted to cover a wide range of situations, they cannot cover all eventualities. Staff using social media and networking sites should avoid any conduct which would lead any reasonable person to question their motives and intentions.

(iv) The school understands that employees have the right to a private life and would respect this so long as employees follow the guidelines set out in this document and other documents they refer to. The school expects employees to maintain reasonable standards in their own behaviour such that enable them to maintain an effective learning environment and also to uphold public trust and confidence in them and their profession. Employees should avoid any conduct which is likely to bring the school into disrepute.

2. Scope

(i) This document applies to all staff who work in the school. This includes all teaching and non-teaching staff. The general principles set out should also be followed by adults who work at the school but are not employed by the school.

(ii) For the purpose of these guidelines, social media and social networking sites are websites by which personal information or opinions can be presented for public consumption and websites which allow people to interact with each other. Examples of social media and social networking sites with internet presence include blogs, Facebook, Twitter, YouTube, Instagram, TikTok, Pinterest, Flickr and Tumblr. Please note that this list is not exhaustive as new technology is emerging on a daily basis but it seeks to provide examples to staff. The definition of social networking and media may be increased as new technologies emerge.

3. Staff guidelines in relation to social networking and media activity

(i) If you wish to have a social media presence, please make sure that your employer is not identified on this presence unless there is, on an objective assessment, a legitimate reason for doing so and ensure that comments made are from your own behalf, for example by writing in the first person and using a personal email address as opposed to your employer's email address.

(ii) Staff are personally responsible for their communication in social media. This includes any media attachments like photographs or videos. What staff publish on a social media site will be available for any member of the public to read (including parents, members of the Governing Body/Trust, colleagues, members of the Local Authority and prospective employers) for a long time. Staff should always think carefully about this when posting personal content.

(iii) Staff should not post any media attachments such as photographs or videos which have subjects (students/colleagues etc.) of the school in them. If you wish to post such items you should always speak to the Principal in the first instance.

(iv) Staff should not place any information regarding their employer, their colleagues, students or people they come into contact with as part of their employment on a social networking or media site.

(v) Staff are advised for their own protection not to put personal information such as home addresses or personal telephone numbers on a social networking or media site.

4. Staff guidelines in relation to student contact

(i) Staff are not expected to interact with any student (or past student under the age of 18) of the school on a social media or networking site. For example, the school would not think it appropriate for staff to accept a friend request from a student or request that a student 'befriend' them.

(ii) Any electronic communication regarding the school or the work you are carrying out in the school (including telephone and text messaging contact) with students or parents/carers should only take place using the school's formal communication systems. Staff should only use the school's website; the school's email address, Bromcom, Satchel One (Show My Homework) or the school's telephone number when

communicating with students and parents/carers. There may be exceptional circumstances (e.g. COVID-19 School Closure) where communication via personal mobile phones of home phones are required in such circumstances staff should always withhold their number before making any calls.

(iii) Staff should not post remarks or comments on-line or engage in online activities which may bring the school into disrepute.

5. Social media and networking sites and cyberbullying

(i) Staff should never use social media to abuse or bully or otherwise comment about colleagues, students, carers of the students or anyone associated in the wide context of the school (e.g. member of the Governing Body/Trust, Local Authority, sponsor etc.). Staff are expected to act respectfully when using social media and to avoid language which may be deemed as offensive to other people. For example, the school would not expect to:

- post anything that could be construed as discriminatory
- post anything that could be construed as racist
- post anything that is untrue or misleading
- post anything that engages in criminal activity
- post anything that is defamatory about people or organisations

(ii) Staff who feel that they are subject to social media bullying by another member of staff or a student should where possible save evidence (e.g. emails, screen prints, text messages) and immediately report this to the Principal for further investigation. Where the complaint is against the Principal, the concern should be raised with the Chair of the Governing Body for further investigation.

iii) Staff who feel that a colleague is not adhering to these guidelines should report their concerns to the Principal for further investigation. Where the complaint is against the Principal, the concern should be raised with the Chair of the Governing Body for further investigation.

APPENDIX Bi: PROTOCOLS FOR THE USE OF MICROSOFT TEAMS – FOR STUDENTS

1. Students must wear suitable clothing; school uniform is not required but revealing clothing or nightwear must not be worn
2. Computers/devices must be used in an appropriate communal area of the home, for example, not in bedrooms; and where possible should be against a neutral background with no other distractions such as TV, music, video game
3. Language must be appropriate, including that of any family members in the background

Student video will be turned off by the teacher/ or the call ended for that student should protocol 1, 2 or 3 not be met and parents will be contacted
4. Student microphones will be muted and managed by the teacher to ensure all students can be heard and are able to contribute
5. Messages typed within the chat feature must be appropriate and written in formal English as would be used in school work – slang or abbreviations should not be used
6. Students should not record or share the meeting in any way
7. Students should not invite other members of their household to join or be involved in the call – this includes younger siblings and parents
8. Students should not ask for or expect individual on-line appointments/meetings with a teacher
9. Students should not attempt to use Teams to message or communicate with other students outside of their scheduled meetings – all activity within Teams is monitored
10. Students should leave the meeting when asked to end the call by their teacher and should not try to remain on the call
11. If students or parents have any concerns they should report this to safeguarding@hayes.bromley.sch.uk

APPENDIX Bii: PROTOCOLS FOR THE USE OF MICROSOFT TEAMS – FOR STAFF

Staff should:
- Ensure they and students must wear suitable clothing, as should anyone else in the household
- Ensure computers/devices used should be in appropriate communal areas of the home, for example, not in bedrooms; and where possible be against a neutral background
- Language used is professional and appropriate, including any family members in the background
- Remain in one place for the duration of the call
- Keep calls to the scheduled length and end them for the entire group at the same time making sure you are the last to leave!
- Remember that safeguarding is just as important when engaging via video call as it is when teaching face to face
- Ensure Safeguarding concerns should be reported in the normal way

Should not**:**
- Meet with an individual student
- Use a private / personal Microsoft Teams/365 account
- Share non-professional content or personal opinions / comments
- Use this as a vehicle to make contact or engage with parents
- Make contact with any student for whom we do not have TEAMS parental permissions
- Use any other video conferencing tools to communicate with students other than your school Teams account
- Record or share the meeting in any way
- Invite other members of a student's household to participate in the call

APPENDIX C: Glossary of terms and abbreviations used

1. CEOP: Child Exploitation and Online Protection is a command of the UK's National Crime Agency, and is tasked to work both nationally and internationally with keeping children safe online

2. TIO: Turn It On are the company which currently provide the school's ICT network support.
3. Windows Defender: Anti-virus software installed on machines and servers within school to ensure the network is protected from viruses, spyware and malware.
4. ICT – Information and Communications Technology
5. Lightspeed: This is a proxy server which filters internet access to prevent inappropriate material being seen in school and monitors web activity of all school users on the school network (both wireless and wired internet use)
6. NSPCC: National Society for the Prevention of Cruelty to Children, this is a charity based in the UK which works to keep children safe
7. Securus: Software which monitors language and activity online and it able to detect and flag the use inappropriate language or content to the school's ICT support team.
8. Bromcom: The school's database containing records of colleague, student and parent details.
9. VoIP: Voice over Internet Protocol, all video conferencing in the school uses VoIP through Skype.

APPENDIX D Acceptable Use Policy

ICT – Acceptable Use Policy

The school has a range of IT facilities and equipment with access to the Internet, a range of software and other resources to support students learning. Our acceptable use policy set out the conditions and rules students should follow when using IT equipment or accessing school platforms. If a student fails to meet these expectations, their user areas will be disabled and the school's behavior management policy will be followed.

The following rules will help keep everyone safe when using these resources.

1. Students will report any computer faults they find immediately to a member of staff.
2. Students will treat the ICT resources with respect, leaving them as they would expect to find them.
3. Students must ask permission from a member of staff before using ICT resources.
4. Students will use only their own log in name and will keep their password a secret. Students will not access other people's accounts or files.
5. In the event that a student moves away from the computer they are logged on to they should lock access to prevent any misuse by others.
6. Students may use the school's ICT resources ONLY for school work.
7. Emails sent from school must be polite and sensible.
8. Students are expected to follow E-Safety guidance and should not disclose their personal details (such as their phone number or address), or the personal details of anyone else whilst using the internet.
9. Students should tell a teacher about anything they see on the computer, which they are unhappy about, or if they receive messages that are of concern.
10. Students may not use their ICT facilities to use/create/distribute offensive material.
11. Students must not attempt to circumvent school ICT security systems.
12. The school will monitor the contents of personal directories and keep a check on Internet sites visited by students