



HPP

Online Safety Policy

This policy was reviewed:	Summer 2025
This policy will be reviewed again:	Summer 2026 <ul style="list-style-type: none">• Additional information on AI added as appendix• Additional information added on pupil mobile phones.
Governor Committee Responsibility:	School Improvement
Statutory policy?	No
Source:	School

Introduction

Key People/dates

 The logo for Hampton Primary Partnership features stylized human figures in green and red, with the text 'Hampton Primary Partnership' to the right.	Designated Safeguarding Lead (DSL) team	Anna Gale (HISN), Jon James (HJS)
	Delegated Online-safety leads	Catherine Clarkson (HISN), Kelsey Farrell (HJS)
	Online-safety / safeguarding link governor	Emily Boswell and Polly Davies
	PSHE/RSHE lead	Sarah Da Silva (HISN), Thea Woolf (HJS)
	Network manager / other technical support	Click on IT
	Date this policy was reviewed and by whom	May 2025 by Jon James, Claire Cook, Kelsey Farrell and Catherine Clarkson
	Date of next review and by whom	Summer 2025 by Kelsey Farrell and Catherine Clarkson

Contents

1. Aims	3
2. Legislation and guidance	4
3. Roles and responsibilities	4
4. Educating pupils about online safety	7
5. Educating parents/carers about online safety	8
6. Cyber-bullying	8
7. Acceptable use of the internet in school	10
8. Pupils using mobile devices in school	10
9. Staff using work devices outside school	11
10. How the school will respond to issues of misuse	11
11. Training	11
12. Monitoring arrangements	12
13. Links with other policies	12
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	13
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)	14
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)	15
Appendix 4: online safety training needs – self-audit for staff	16
Appendix 5: online safety incident report log	17

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key 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, antisemitism, 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 scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

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

By providing support and challenge to the ELT, Governors ensure that

- 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 coordinate 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. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers 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)
- reassure themselves that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and procedures
- reassure themselves that HPP, 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

3.2 The Executive Headteacher (EHT)

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

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and 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 EHT in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the EHT and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Providing regular online safety, 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
- 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 (Click on it) to make sure the appropriate systems and processes are in place
- Working with the EHT, 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
- Ensuring that any online safety incidents are logged (CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the EHT
- Undertaking annual risk assessments that consider and reflect the risks children face

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Ensure that the LGfL filters are robust and effective. Any request to unblock a website is first qualified to ensure the site is safe.
- Ensure that the default LGfL filtering blocked categories are enforced.
- Work with the School DSLs to setup scheduled reporting via the LGfL Webscreen system. This involves the school's DSLs receiving a report from LGfL once a week listing any visit attempts to websites within the PREVENT or ADULT categories groups. Please note that the LGfL filters are not a proactive reporting tool. Whilst they are very good at blocking most unsuitable sites, they do not have a system to alert you of these attempts. The only reports are reactive and are run at the end of the week.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

3.5 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 or processes failing by raising a ticket with CITL.
- Following the correct procedures by logging into the LGFL filtering system 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.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of School 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 1 and 2)

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](#)

3.7 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 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website and weekly newsletter. This policy will also be shared with parents/carers.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of school and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the ELT.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power (see also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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 pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The ELT, and any member of staff authorised to do so by the ELT (as set out in your 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 pupils, 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 pupils and staff. If the search is not urgent, they will seek advice from the EHT or 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 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 executive headteacher or DSL 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/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 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

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

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

As of September 2025, the following updates have been made to the HPP Online safety policy in regards to our expectations and procedures of mobile devices on the school premises. From this date, the school will align with the Richmond Borough agreement outlined in the letter found in Appendix 1 which states that **'we are committed to making our schools smartphone free. Children cannot use smartphones during school hours and we do not want your child to bring a smartphone into school'** .

To support the success of this initiative, the following will be school policy:

- Only children in year 5 and 6 will be allowed to bring mobile phones into school.
- Parents wishing their child to bring a phone will be required to complete the Mobile Phone eform, giving permission for their child to bring a phone to school and sign the agreement.
- Mobile phone eform: <https://forms.gle/9XzXVzMJftBgtDV9>
- **Feature phones or 'brick phones'** will be automatically accepted. These are phones with basic functionality and do not have access to the internet or social media. This feature / brick phone must be powered off prior to entering the school site and immediately handed into the class teacher. These phones do not need to be handed in to the school office. Pupils will have no access to them whilst they are on school premises. Examples of feature / brick phones can be found in Appendix 2.
- **Smartphones** are not permitted unless there are exceptional circumstance. The specific reason will need to be indicated on the eForm and a compulsory meeting with a member of the Executive Leadership Team is required before any agreement is made. The following reasons maybe considered:
 1. The child has a medical condition that requires a smartphone device
 2. The child is required to travel independently to and from school using public transport
- If approved, the smartphone must be powered off prior to entering the school site and immediately handed into the school office where it can be collected at the end of the day.

This process will be monitored by a senior leader to ensure that only agreed smartphones are being brought to school. Pupils will have no access to them whilst they are on school premises.

- **Smart watches** will not be permitted at school.
- Parents / adults are not permitted to use mobile phone devices on the school playground during the school day. Any adult using a mobile device will be asked to end the call or leave the site to finish the call. Signs will be placed around the school site to remind parents.
- During assemblies / events in school, parents are able to take images of their child but these must not be uploaded to any form of social media.
- Any breach of the Mobile Phone agreement by a pupil will trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device. This includes failure to hand the device in on arrival to school.

GPS Trackers

As a school, we strongly discourage the use of tracking devices with children of any age. However, we appreciate that some parents may have concerns once their child reaches an age to walk to/from school independently. If you do decide to provide your child (Year 6 only) with a GPS tracking device (such as AngelSense or Gabb Watch), these will be treated in the same way as a mobile phone. Children will be required to turn them off and hand them in upon arrival at school. They will not have access to them until the end of the day.

Bluetooth tracking systems (such as AirTag, Galaxy SmartTag2 and Tile) are not permitted in school. Their presence can cause false stalking alerts and make it difficult for the school to effectively safeguard all children and staff.

No form of GPS or Bluetooth tracking device is permitted on school excursions.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from CITL.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This will be captured on CPOMS.

This policy will be reviewed every year by the ICT manager. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I select a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use my phone on the school site unless given permission by a staff member
- Parents will complete the mobile phone consent form prior to me bringing it into school
- I will always hand my phone in to the class teacher at the beginning of the day
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Signed (parent/carer):

Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5 in the Online Safety Policy

1. Statement of intent for the use of AI

At Hampton Primary Partnership (HPP), we recognise that the use of artificial intelligence (AI) can help to positively affect teacher workload, develop pupils' intellectual capabilities and prepare them for how emerging technologies will change workplaces, education and leisure. While there are benefits to the use of AI tools, the content they produce may not always be accurate, safe or appropriate and could lead to malpractice.

Through the measures outlined in this statement, the school aims to ensure that AI is used effectively, safely and appropriately to deliver excellent education that prepares our pupils to contribute to society and the future workplace.

For the purposes of this statement, the following terms are defined as:

- **AI** – The theory and development of computer systems able to perform tasks normally requiring human intelligence
- **Generative AI** – A category of AI algorithms that generate new outputs based on the data they have been trained on.
- **Misuse of AI** – Any use of AI which means that pupils have not independently demonstrated their own attainment

2. Legal framework

This statement has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Generative artificial intelligence in education'
- DfE (2023) 'Meeting digital and technology standards in schools and colleges'
- JCQ (2023) 'Artificial Intelligence (AI) Use in Assessments: Protecting the Integrity of Qualifications'
- JCQ (2023) 'Suspected Malpractice Policies and Procedures'

This policy operates in conjunction with the following school policies:

- Online Safety Policy
- Cyber-security Policy
- Data Protection Policy

- Child Protection and Safeguarding Policy
- Acceptable Use Agreement

3. Roles and responsibilities

The ELT will be responsible for:

- Ensuring that this statement is effective and complies with relevant laws and statutory guidance.
- Reviewing this statement as part of the Online Safety Policy
- Ensuring their own knowledge of the use of AI tools in the school is up-to-date.
- Ensuring all staff undergo child protection and safeguarding training, including online safety, at induction and at regular intervals.
- Ensuring the school follows the DfE's digital and technology standards.
- Ensuring that the use of AI tools in the school is integrated into relevant policies and procedures, the curriculum and staff training.
- Communicating with parents to ensure they are kept up-to-date with how AI tools are being used in the school, how this will impact pupils' education and how the school is ensuring the tools are being used safely and effectively.
- Working with the Computing lead and school DSL to review and update this statement on an annual basis.
- Ensuring that AI practices are audited and evaluated on a regular basis.

ICT support will be responsible for:

- Providing technical support in the development and implementation of the school's AI practices, policies and procedures.
- Implementing appropriate security measures.

The DPO will be responsible for:

- Understanding and maintaining awareness of what the use of AI means for data protection in the school.
- Advising the school on how to integrate the use of AI while complying with data protection regulations.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in school.
- Undertaking training so they understand the risks associated with using AI tools in school.
- Liaising with relevant members of staff on online safety matters.
- Maintaining records of reported online safety concerns relating to the use of AI tools, as well as the actions taken in response to concerns.

All staff members will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Taking responsibility for the security of the AI tools and data they use or have access to.
- Modelling good online behaviours when using AI tools.
- Maintaining a professional level of conduct in their use of AI tools.
- Having an awareness of the risks that using AI tools in school poses.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring that the safe and effective use of AI tools is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from the relevant school staff if they are concerned about an experience that they or a peer has experienced while using AI tools.
- Reporting concerns in line with the school's reporting procedure.
- Familiarising themselves with any AI tools used by the school and the risks they pose.

4. Data protection and cyber-security

The school is aware of the data privacy and cyber-security implications that come with using generative AI tools and will ensure that all AI tools are used in line with the school's Data Protection Policy and Cyber-security Policy. The school will follow the procedures in these policies to continue to protect pupils from harmful online content that could be produced by AI tools.

The school will not enter data that is classed as personal and sensitive into public AI tools under any circumstances. Any data entered will not be identifiable and will be considered released to the internet.

Free AI tools may process and store data using global infrastructure that falls outside UK GDPR jurisdiction. Submitting any Personally Identifiable Information (PII), sensitive school data, or identifiable student/staff content can lead to data protection breaches.

Content entered into free AI platforms may be used to train future models. This means that anything submitted – even accidentally – could theoretically become part of a future public dataset.

The school will:

- Protect personal and special category data in accordance with data protection legislation.
- Not allow or cause intellectual property, including pupils' work, to be used to train generative AI models, without appropriate consent or exemption to copyright.
- Review and strengthen cyber security by referring to the DfE's cyber standards.
- Be mindful that generative AI could increase the sophistication and credibility of cyber attacks.
- Ensure that pupils are not accessing or creating harmful or inappropriate content online, including through AI tools.
- Refer to the DfE's [Filtering and monitoring standards for schools and colleges](#) to ensure that the appropriate systems are in place.
- Be mindful of the data privacy implications when using AI tools and will take steps to ensure that personal and special category data is protected in accordance with data protection legislation.

If it is necessary to use personal and special category data in AI tools, the school will ensure that the tools comply with data protection legislation and existing privacy policies to protect the data.

The school will be open and transparent whilst ensuring that data subjects understand their personal or special category data is being processed using AI tools.

5. Using AI tools

The school will ensure that AI tools are used appropriately to achieve the following aims:

- To reduce workload
- To free up teachers' time
- To assist with the production of high-quality and compliant administrative plans, policies and documents
- To support the teaching of a knowledge-rich computing curriculum
- To teach pupils:
 - How to use emerging technologies safely and appropriately.
 - About the limitations, reliability and potential bias of AI tools.

How information on the internet is organised and ranked.

How online safety practices can protect against harmful and misleading content.

To identify and use appropriate resources to support their education, including age-appropriate resources and preventing over-reliance on a limited number of tools or resources.

Whilst recognising that AI tools can be used appropriately and with benefit to teaching and learning, the school will keep in mind that the content produced by AI tools can be:

- Inaccurate.
- Inappropriate.
- Biased.
- Taken out of context and without permission.
- Out of date or unreliable.

Where AI tools are used, all staff members will understand that the quality and content of the final document remains the professional responsibility of the staff member who produced it. Staff members using AI tools to create documents will not assume that AI output will be comparable with a human-designed document that has been developed in the specific context of the school.

Staff members will be aware that AI tools return results based on the dataset it has been trained on – it may not have been trained on the national curriculum, and may not provide results that are comparable with a human-designed resource developed in the context of the national curriculum. Staff members will be mindful of this in their teaching and marking of pupils' work.

Pupils and staff members will be reminded that using AI tools cannot replace the judgement and deep subject knowledge of a human expert. Staff members will stress the importance of pupils acquiring their own knowledge, expertise and intellectual capability rather than relying on AI tools in their work.

The school will not allow or cause pupils' original work to be used to train AI tools.

6. AI awareness

Guidance from ClickonIT:

Always anonymise any data before entering it – never include names, email addresses, UPNs, or staff/student details

1. Avoid entering confidential or sensitive content – if it feels like private information, don't type it in
2. Treat the AI like the public internet – assume anything you enter could be stored or viewed
3. Double-check all AI-generated content for accuracy, bias, and appropriateness
4. Do not upload files or documents containing internal or protected data

Staff members will be aware of and look out for potential indicators of AI use, which include:

- A default use of American spelling, currency, terms and other localisations.

- A default use of language or vocabulary which might not appropriate to the working or qualification level.
- A lack of direct quotations and/or use of references where these are required or expected.
- Inclusion of references which cannot be found or verified.
- A lack of reference to events occurring after a certain date, reflecting when an AI tool's data source was compiled.
- Instances of incorrect or inconsistent use of first-person and third-person perspective where AI generated text has been left unaltered.
- A variation in the style of language evidenced in a piece of work, if a pupil has taken specific portions of text from an AI tool and then amended it.
- A lack of graphs, data tables or visual aids where these would normally be expected.
- A lack of specific, local or topical knowledge.
- Content being more generic in nature.
- The inadvertent inclusion of warnings or provisos produced by AI tools to highlight the limits of its ability or the hypothetical nature of its output.
- The submission of pupil work in a typed format, where this is not usual, expected or required.
- The unusual use of several concluding statements throughout the text, or several repetitions of an overarching essay structure within a single lengthy essay.
- The inclusion of confidently incorrect statements within otherwise cohesive content.

Staff members will remain aware that AI tools can be instructed to employ different languages and levels of proficiency when generating content, and some are able to produce quotations and references.

7. Safeguarding

The school acknowledges that generative AI tools can be used to produce content that is dangerous, harmful, and inappropriate. The school will follow the procedures set out in the Child Protection and Safeguarding Policy and the Online Safety Policy to ensure that pupils are not able to access or be exposed to harmful content.

HPP 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.

HPP will treat any use of AI to bully pupils in line with our behaviour policy.

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.

Pupils will be taught about the risks of using AI tools and how to use them safely. Pupils will be made aware of how to report any concerns or incidents involving generative AI, and who to talk to about any issues regarding the use of AI tools.

The school will ensure that parents are aware of who to speak to about any concerns or issues regarding the use of AI.

The school will ensure that the appropriate filtering and monitoring systems are in place to protect pupils online, following the DfE's [filtering and monitoring standards](#).

All staff members will receive training on the safe use of AI as part of their online safety training, which is regularly updated.

8. Teaching pupils about the safe use of AI

Teaching about the safe and appropriate use of AI will ensure that pupils benefit from a knowledge-rich curriculum which enables them to become well-informed users of technology and understand its impact on society. Pupils will gain strong foundational knowledge which ensures they are developing the right skills to make the best use of AI tools.

The school will:

- Teach pupils how to use emerging technologies, including AI tools, safely and appropriately.
- Raise awareness of the limitations, reliability and potential bias of AI tools.
- Help pupils to understand how information on the internet is organised and ranked.
- Include online safety teaching in the curriculum and how to protect against harmful or misleading content.
- Raise awareness and understanding of protecting intellectual property rights.
- Encourage the safe and responsible use of digital content.
- Teach about the impact of technology, including disruptive and enabling technologies.

Pupils will be supported to identify and use appropriate resources to support their ongoing education through the use of age-appropriate resources, which may include AI tools, whilst preventing over-reliance on a limited number of tools or resources

9. Fraudulent emails / information

Our school may also be targeted by fraudulent emails, such as 'phishing' attacks, which are often AI-generated and very convincing. Look out for the following signs:

- Email addresses that don't match the contact details you have on file
- Poor spelling and grammar, including American spellings, or an overly formal tone
- Messages demanding urgent, time-sensitive action

- Suspicious links, e.g. containing strings of numbers
- Generic introductions (e.g. Dear Sir or Madam)

Report any suspicious emails to our data protection officer (DPO), the Federation Business Manager.

Appendix 1: Letter from Richmond - Smartphone use in school

July 2024

Dear Parents/Guardians,

A Joint Statement on a Smartphone-free Childhood by Richmond Primary School Headteachers

As you may have seen on social media and news coverage recently, there is a growing movement amongst parents to support a campaign called “Smartphone Free Childhood”. We, the undersigned Headteachers of primary schools in the London Borough of Richmond, think it is an important safeguarding and wellbeing issue that we want to bring to your attention. You can find out more by visiting these links:

<https://smartphonefreechildhood.co.uk/schools-guide>

<https://delaysmartphones.org.uk/evidence/>

The Smartphone Free Childhood campaign has been discussed at length in our Richmond Primary Heads’ Network Meeting, and a significant number of our primary schools in the Borough are keen to support it in any way that we can. By “smartphones”, we refer to phones that are able to access the internet, as opposed to mobile phones that can only text and make phone calls. The dangers with smartphones to children come specifically from social media apps and unsupervised internet use.

We understand the importance of being able to contact your child as they become more independent - walking to and from school - in order to give you peace of mind, and for children to be able to call in emergencies. However, while children need to be contactable, their phones do not need to have access to the internet in order for you to keep them safe.

While smartphones can be a very helpful piece of technology for adults, they can expose children to a number of negative risks. Research now tells us that smartphones:

- have been linked to poor mental health, depression and low self-esteem, especially in young teenagers (*National Library of Medicine*, 2019)
- expose children to harmful content including pornography, grooming, bullying and materials that are not age appropriate (*Canadian Medical Association Journal*, 2020)
- reduce attention spans - they are changing the way children’s brains develop and fundamentally affecting their ability to concentrate (*National Commission for Protection of Child Rights*, 2021)
- Deprive children of their childhood - time spent on a device reduces time spent playing, interacting and developing vital social skills (*The Anxious Generation* by Prof Jonathan Haidt, 2024)
- are highly addictive, with lasting effects on young and developing brains being similar to that of gambling (*Pew Research Centre*, 2022)

The use of smartphones is now a feature of daily life for most adults. Yet, over the last few years the age at which children are given their first smartphones has dropped significantly. According to recent research, some alarming figures tell us that:

- a fifth of 3-4 year olds in the UK have a smartphone (*The Guardian*, 19 Apr 2024)
- almost a quarter of 5-7 year olds have a smartphone (*Ofcom*, 19 April 2024)
- 91% of 11 year olds have a smartphone (*The Guardian*, 1 Feb 2024)

To show our professional support for this campaign, we support and encourage the campaign for parents to delay giving their child a smartphone until they reach the age of 14, opting instead for a text/call phone or alternative if necessary. We believe we can all work together across Richmond schools and join the growing movement across the country to change the 'normal' age that children are given smartphones.

In May 2024, St Albans was the first town in the UK to declare its intention to go smartphone-free for under 14s. Our two local MPs - Sarah Olney (Richmond) and Munira Wilson (Twickenham) - have been contacted about this issue more than any other MPs across the UK in recent months, which signals to us an appetite within our community to follow suit.

To be successful, this movement relies on you, our children's parents and carers, to resist the pressure from your children and their peers, and hold back on giving your children smartphones until they are 14. In this way you will be working together with a wide network of parents and schools to reset the expectations that children should have access to a smartphone, and remove the social peer pressure to do so.

If you would like to find out more about this issue (including the facts listed above and alternative phone options) or would like to become more actively involved, please visit this link, which will lead you to the national linktree for this campaign, where you can also find your local school group: <https://linktr.ee/smartphonefreechildhood>

The future of the children in our Borough is paramount to us all. In a world where fast-changing technology is impacting the development of our children's brains, it is up to us to promote a cultural change that will allow children to flourish safely and away from harm.

Yours faithfully,

Richmond Primary Headteachers

Appendix 2: Examples of feature / brick phones



Nokia 3210



Nokia 2660



Dora 6820