Feltham Hill
Infant and Nursery School

# Online Safety Policy

Pupils must be protected online and kept safe from harm.
This policy identifies clear procedures to support pupils at risk.
And identifies teaching online safety.

## November 2023

*Prepared by: Headteacher Nov 2023*
*Discussed with: Strategy team & SBM Nov 2023*
*Shared with staff: Nov 2023*
*Agreed with: Safeguarding governor/Chair and FGB Nov 2023*
*To be reviewed: Nov 2024*

**Aims**

**The 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 leaders to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

**The 4 key categories of risk**

School's 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.

**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
- 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.

**Roles and responsibilities**

**The governing body**

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

- Governors alongside the Headteacher/Designated safeguarding lead (DSL)) 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.
- Governors alongside the Headteacher/DSL will also make sure all staff receive regular online safety updates, as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

- The named safeguarding governor/chair of full governing body (FGB) will have a termly safeguarding focus visit with the Headteacher/DSL) to discuss and monitor online safety, as part of the safeguarding report.
  This governor is Jane Kendall-Nicholas.

- Governors alongside the Headteacher, personal social health education (PSHE) lead and senior leadership team (SLT) mentor, will ensure children are taught how to keep themselves and others safe, including keeping safe online.
- Governors alongside the school business manager (SBM) and deputy Headteacher (DH)/safeguarding deputy will ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.

Governors alongside the SBM and DH/safeguarding deputy will review the DfE filtering and monitoring standards, and discuss with schools' Hounslow Information technology (IT) service provider what needs to be done to support the school in meeting those 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.

In addition, all governors will:

- Ensure they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's information communication technology (ICT) systems and the internet using iAM Compliant. (Appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures, alongside the Headteacher/DSL.
- 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), alongside the Headteacher/DSL and special educational needs co-ordinator (SENCo).
- 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

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

**The designated safeguarding lead (DSL)/Headteacher**
Details of the role of the school's DSL and two deputies, are set out in school's child protection and safeguarding policy, as well as, their names displayed around the school.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the strategy team and governors to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.

- Supporting 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 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 or directing staff to relevant Hounslow courses.
- Liaising with other agencies and/or external services if necessary.
- Providing regular termly reports on online safety in school to the named safeguarding governor/chair FGB.
- 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 will be on the first in-service-education and training (INSET) day in September or when staff join the school.

**The school business manager (SBM) with the deputy Headteacher (DH)/safeguarding deputy**
Will:

- Understand the filtering and monitoring systems and processes in place on school devices and school networks.
- Work with Hounslow ICT manager to make sure the appropriate systems and processes are in place.

**Deputy Headteacher (DH)/safeguarding deputy**

- The DH leads the key stage 1 (KS1) curriculum, alongside subject leaders.
- Alongside, the Computing lead, they plan online safety to be used during all computing lessons using the internet.
- Also, pupils learn about being safe on the National safer internet day which is part of online safety week.
- Pupils learn not to share their details with anyone online. As they may not know who they are talking to.

**ICT consultant**
The ICT consultant alongside the SBM and Computing lead 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.

**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, and ensuring that pupils follow the school's terms on acceptable use using iAM compliant.
- (appendix 2)
  Knowing that the deputy DSL/DH alongside the SBM 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 emailing the office.
- Following the correct procedures by emailing the SBM and DH/safeguarding deputy if they need to bypass the filtering and monitoring systems for educational purposes.

- Working with the DSL/Headteacher 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.'

**Parents/carers**
Parents/carers are expected to:

- Notify a member of staff or DH or the Headteacher of any concerns or queries regarding this policy.
- Sign an agreement for acceptable use of ICT on their child's admission form. (appendix 1)

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 International
- Parent resource sheet – Childnet International

**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 of ICT using iAM Compliant.
(appendix 2)

**Educating pupils about online safety**
Pupils will be taught about online, safety as part of the curriculum:

- The curriculum is taken from the National Curriculum computing programmes of study.
- It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.
- Computing and PSHE and RHE lessons are taught weekly in KS1.During Computer lessons there is a pupil adult ratio of 1:15 with the other half the class in the Library.
- This is to support online safety.

Schools have to teach:
Relationships education and health education in primary schools.

In **KS1**, 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.

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.

**Educating parents/carers about online safety**
Parents/carers will be reminded that their children must not be online at home unsupervised and should be in a room with an adult.
They will be reminded to have control settings, at home and monitor what site their child is using.

- In addition, the school will raise parents/carers' awareness of internet safety in emails or newsletters where necessary, and in information via the website.
- This policy will also be shared with parents/carers.
- Online safety will also be covered during new parents' information meetings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access.

- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the DH/safeguarding deputy.
- Concerns or queries about this policy can be raised with the DH/safeguarding deputy or the Headteacher.

**Cyber-bullying**
**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 the school's behaviour including anti-bullying policy.)

**Preventing and addressing cyber-bullying**
Parents/carers will be reminded about always supervising their child at home, when online.

In addition:

- Leaders will ensure that pupils understand what cyber-bullying is and what to do if they become aware of it happening to them or others.
- That they 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 discuss cyber-bullying with pupils, using an appropriate language for their age.
- Teacher will discuss cyber-bullying with their classes, when necessary.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.
- This includes 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.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

- If 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.

**Examining electronic devices**
The pupils are too young, to have mobile devices, so they would not be allowed to bring them to school.

However, it is important for leaders to know the legal position for harmful content.

The Headteacher/DSL, or a member of the strategy team 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 evidence in relation to an offence.

Before a search, if the Headteacher/DSL, or a member of the strategy team 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.
- 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.
- The Headteacher/DSL, or a member of the strategy team 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 Headteacher/DSL, with a member of the strategy team to decide on a suitable response.
- If there are images, data or files on the device that the Headteacher/DSL reasonably suspects 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, the Headteacher/DSL, with a member of the strategy team 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, the Headteacher/DSL, with a member of the strategy team 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 Headteacher/DSL immediately, who will decide what to do next.
- The Headteacher/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

**Artificial intelligence (AI)**

In the school, Computing lessons are supervised.
Also, research online for other subjects will be in busy learning areas, so pupils can be supervised.

- Within the family, generative artificial intelligence (AI) tools are now widespread and easy to access.

- Parents/carers may be familiar with generative chatbots, such as, ChatGPT and Google Bard.

- Staff should be aware of the risks of using AI tools whilst they are still being developed and the SBM alongside the Computing lead, should carry out a risk assessment where new AI tools are being used when necessary.

**Acceptable use of the internet in school**
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 using iAM Compliant.
(appendix 2)

- 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.
- Leaders 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.

**Pupils using mobile devices in school**
Pupils may not bring mobile devices into school, as they are too young.

**Staff using work devices outside school**

- All teachers 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.

And the ICT consultant:

- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

- Teachers must not use the device in any way that would violate the school's terms of acceptable use, as set out.
- 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 the SBM who will contact the ICT consultant.

**How the school will respond to issues of misuse**
A pupil in the school is unlikely to misuse the school's ICT systems or internet, as they are always supervised and there are control settings.

- 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, discipline and grievance procedures.

- The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- Leaders will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**Training**
All new staff members will receive training, as part of their induction, on safer 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, this will be on the first INSET day in September.
- Staff will also receive relevant updates as required (for example through emails, e-bulletins and feedback 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, 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/Headteacher and two deputies will undertake child protection and safeguarding Hounslow leader 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 safer internet use and online safeguarding issues, as part of their Hounslow 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.

**Monitoring arrangements**
The DSL/Headteacher will log behaviour and safeguarding issues related to online safety, if they arise.

- This policy will be reviewed every year by the Headteacher/DSL.
- At every review, the policy will be shared with the named safeguarding governor/chair FGM.
- Then agreed with first FGB in November.

- The review 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.

**Links with other policies**

This online safety policy is linked to schools':

- Child protection and safeguarding policy
- Behaviour including anti-bullying policy and statement of behaviour principles
- Staff code of conduct, discipline and grievance procedures
- Privacy notices
- Complaints procedure

**Appendix 1: KS1 acceptable use agreement KS1 parents/carers**

**Acceptable use of ICT KS1 parents/carers**

**On the admission form:**

**Parents will sign to say:**
I give consent for my child to use the school's ICT systems and internet when appropriately supervised by a member of school staff. I will ensure my child knows how to be safe online using the principals of the School's Online Safety Policy found on
www.fhi.hounslow.sch.uk/school-policies

**When using ICT teachers will remind KS1 pupils to:**
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 the teacher immediately if:
They select a website by mistake
Receive messages from people they don't know
Find anything that may upset or harm them or their friends

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 class username and password
Log on with adult support

Never give my personal information (my name, address or telephone numbers) to anyone
Save my work on the school network with help from the teacher
Check with my teacher before I print anything
Log off or shut down a computer when I have finished using it with help from the teacher

**Appendix 2: Shared and agreed through iAM Compliant**

**Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors**

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 which could harm the school's reputation.
- Access social networking sites or chat rooms.
- Use 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.
- 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.
- Infringe any copyright restrictions or intellectual property rights
- Comment negatively on staff, parents, children or any member of the school community in any electronic communications and I will not respond to any comments made about the school in any electronic communications.

***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.
- Ensure that my online activity, both in and outside school, will not bring my professional role or the school into disrepute.
- Only use the school's e-mail system for official school business use and understand that all work related emails remain the property of Feltham Hill Infant and Nursery school.
- Understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- 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.
- Let the designated safeguarding lead (DSL) and ICT Consultant know if a pupil informs me they have found any material which 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.