Online Safety Policy
March 2024

Hugh Joicey C of E School, Ford

Love one another ~ Love learning ~ Love nature

Our school aims to:

- Have robust processes in place to ensure the online safety of all pupils, staff, volunteers and governors
- Identify and support groups of pupils who 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

<u>The 4 key categories of risk</u>

Our approach to online safety is based on addressing these categories of risk.:

1. **Content** - being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism
2. **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
3. **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending or 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 etc.

4. **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

This policy is based on Department for Education's (DfE) 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, but is 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 pupil's electronic devices where they believe there is good reason to do so.
This 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.
The governing body will make sure that all staff undergo online safety training as part of child protection and safeguarding training, and ensure that staff understand the expectations, roles and responsibilities around filtering and monitoring.
The governing body will also make sure that all staff receive regular online safety updates (vis e-bulletins, email and staff meetings) as required and at least annually, to ensure they are continually provided with relevant skills and knowledge to effectively safeguard children.
The governing body 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 body should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The governing body 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 body 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 the safeguarding needs

All governors will:

- Ensure they have read and understood the policy
- Agree and adhere to the terms on the acceptable use of the school's ICT systems and the internet (Acceptable Use Form, available in the school office)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and 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.

<u>The Headteacher</u>

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

<u>The DSL</u>

Details of the DSL (and deputy) are set out in our Child Protection and Safeguarding Policy.

The DSL takes responsibility for online safety in school, including:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing body to review this policy annually and ensure that policies and procedures and implementation are updated and reviewed regularly
- Understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT staff to make sure that the appropriate filtering and monitoring systems are in place
- Working with the headteacher, ICT staff and other staff to address any online safety issues or incidents
- Managing online safety issues and incidents in line with the school's Child Protection and Safeguarding Policy
- Ensuring that any online safety issues and incidents are logged (using the CPOMS system) 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 governing body
- 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 exhaustive.

<u>The ICT Manager</u>

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 ad 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 (using the CPOMS system) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriate in line with the school's behaviour policy

This list is not exhaustive.

<u>All staff and volunteers</u>

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 the acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow these terms.
- 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 using the CPOMS system, or via email/face to face conversation
- Following the correct procedures by directly requesting permission from the headteacher 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 on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying 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 exhaustive.

Parents /carers

Parents /carers are expected to:

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

Parents /carers can seek further guidance on keeping children safe online from the following organisations and websites:
Homepage - UK Safer Internet Centre
Help & advice | Childnet
Keeping children safe online | NSPCC

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.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.
All primary schools have to teach Relationships Education and Health Education.
In Key Stage 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 on the internet or other online technologies

In Key Stage 2, pupils 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 schools, 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 contact and content 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.

Educating parents / carers about online safety
The school will raise parents/carers' awareness of online safety in letters or other communication home, and in information on the school website or Seesaw. This policy will also be shared with parents on the school website.
Online safety will also be covered at parents consultations.
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 and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or DSL.
Concerns or queries about this policy can be raised with the headteacher.

Cyberbullying
Cyberbullying 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 one person or group, by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and the school's anti bullying policy).
Preventing and addressing cyberbullying
To help prevent cyberbullying, 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 cyberbullying with pupils , explaining the reasons why it happens, the forms it may take and what the consequences can be. Class teachers will discuss cyberbullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal , social, health and economic education, and other subjects as appropriate.
All staff, governors and volunteers (as appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training.
The school also sends information leaflets on cyberbullying 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 cyberbullying, 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 it is reasonably practicable, if they have reasonable grounds to suspect that possessing the material is illegal. They will also work with external services if it is deemed necessary to do so.

<u>Examining electronic devices</u>
The headteacher, and any member of staff authorised to do so by the headteacher, 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 headteacher
- 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 if there is 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 to decide on a suitable response. If there are images, data or files on the device that the staff

reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
When deciding if there is 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 in 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 the 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 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 Screening, Searching and Confiscation
- UKCIS guidance on Sharing Nudes and Semi-nudes: Advice for Education Settings Working with Children and Young People
- School 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 procedures.

<u>Artificial Intelligence</u>
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 Chat GPT and Google Bard.
Hugh Joicey C of E First 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 creates images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
Hugh Joicey C of E Aided First School will treat any use of AI to bully pupils in line with our behaviour and anti-bullying 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 bring used by the school.

<u>Acceptable use of the internet</u>

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. 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 to ensure that they comply with the above and restrict access through filtering and monitoring systems where appropriate.
Pupils are not permitted to bring mobile phones to school. If one is brought in e.g. if they are staying at another house over the weekend and need to have a phone there for contact, it will be handed in to the school office and stored safely until the pupil is collected by an adult.

Staff using work devices out of 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 long, with a combination of upper and lower case letters, numbers and special characters
- Ensuring their hard drive is encrypted - this means that 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
- Keep operating systems up to date

Staff members must not use the device in any way that would violate the school's terms of acceptable use.
Work devices must be solely used for work activities.
If staff have any concerns over the security of their device, they must seek advice from the headteacher and the ICT manager.

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 and the acceptable use agreement. 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 internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on 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.

Training

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

All staff members will receive refresher training at least once every academic year as part of safeguarding training, as well as relevant updates as required.

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 group chats
  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 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.

Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety on CPOMS.

The policy will be reviewed every year (or more frequently if there are updates) by the headteacher. At every review, the policy will be shared with the governing body.

Links with other policies

- Child protection and safeguarding
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notice
- Complaints procedures

- ICT and acceptable use policy