Online Safety Policy

September 2021

Review date: September 2022

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Ensure that all stakeholders are clear of their role in safeguarding and promoting the welfare of all children online and know that this is everyone's responsibility.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2021 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/999348/Keeping_children_safe_in_education_2021.pdf and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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 body

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

The governing body will discuss online safety with appropriate staff regularly, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
-

3.2 The Headteacher

The Headteacher is responsible for:

- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Developing, alongside senior leaders, a preventative curriculum ensuring that children are taught about safeguarding, including how to stay safe online and how to identify the signs of online abuse.
- Ensuring that subject leaders include online safety as a running and interrelated theme whilst devising and implementing curricula, policies and procedures.
- Ensuring that staff receive training and guidance on how to identify the early signs of online abuse (including peer on peer abuse).
- Developing a culture where staff feel comfortable to challenge any inappropriate behaviours.
- Ensuring that staff receive advice and training in how to reassure victims that they are being taken seriously and that they will be supported and kept safe.

3.3 The designated safeguarding lead

Details of the school's Headteacher, who is also the Designated Safeguarding Lead (DSL), and Deputies DDSLs are set out in our Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in school (but has delegated the responsibility to the Deputy Designated Safeguarding Lead, Miss Snowball) in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the DDSLs, ICT support team, ICT Leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying, including any reported incidents of abuse via mobile phone, are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering (where appropriate) staff training on online safety, particularly focusing on the four areas of risk:
- **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Sematism, radicalisation and extremism.
- **Contact**: being subjected to harmful online interaction with other users; for example: 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; for example, 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
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing body

This list is not intended to be exhaustive.

3.4 The ICT support team

The ICT support team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
-

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

Delivering a preventative curriculum ensuring that children are taught about safeguarding including how to stay safe online, tackling (in an age-appropriate and inclusive manner) issues such as:

- Healthy, respectful and safe online relationships
- Respectful online behaviour
- Cyberbullying
- Consent
- Gender roles, stereotyping and equality
- Body confidence and self-esteem
- Prejudiced behaviour
- Online gambling, phishing and financial scams
- Content as delivered by the DSL/DDSLs under the four categories of risk

Being aware that children can abuse other children online (often referred to as peer on peer abuse). This can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Being aware of the signs of any form of online abuse (including peer on peer abuse) and highlighting to the DSL/DDSLs and logging any concerns that they have through the usual safeguarding procedures.

- Ensuring that any incidents of cyber-bullying (including peer on peer abuse) are dealt with appropriately in line with the school's safeguarding and behaviour policies.

Challenging inappropriate behaviours between peers, that are abusive in nature. Staff must not downplay certain behaviours, for example dismissing sexual harassment as "just banter", "just having a laugh", "part of growing up" or "boys being boys". This can lead to a culture of unacceptable behaviours, an unsafe environment for children and in worst-case scenarios a culture that normalises abuse, leading to children accepting it as normal and not coming forward to report it.

- Reassuring victims that they are being taken seriously and that they will be supported and kept safe.

Staff should understand that even if there are no reports of online abuse (including peer on peer abuse) it does not mean that it is not happening, it may be the case that it is just not being reported. As such, if staff have any concerns regarding peer on peer abuse they should speak to their designated safeguarding lead (or deputy).

- 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.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy

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

- What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
-

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.

4. Educating pupils about online safety

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

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

- Use technology safely and respectfully, keeping personal information private.
- Understand the rules of 'stranger danger' when linked to online use.

- Be responsible online citizens by being respectful to others.
- 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 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour (including peer on peer abuse).
- Identify a range of ways to report concerns about content and contact.

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. Online safety is also discussed throughout all areas of the curriculum by class teachers.

In the summer term, Year 5 & 6 children receive a discretely taught series of sessions using a PREVENT based online training platform. This teaching enables children to make sensible choices when online. It will also help to be aware of the flags and triggers to look out for in order to protect themselves against becoming targets for terrorism, radicalisation, patriotism and grooming, particularly when using the internet or other ICT systems.

By the end of their primary education, 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.

5. Educating parents about online safety

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

Online safety where necessary will also be covered during parents' evenings.
E-Safety newsletters including pertinent information are created by the SLT and sent home.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/DSL, Deputy Headteacher/DDSL or the Assistant Headteacher/DDSL.

Concerns or queries about this policy should also be raised with the Headteacher.

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 one person or group by another person or group, where the relationship involves an imbalance of power.

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. Class teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies at an appropriate level of content for all children.

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.

6.3 Term time online learning from home

At weekends, when completing homework, and under other exceptional circumstances, such as school closures due to extreme weather, children may be expected to work online from home.

Teachers may set work for children via specific secure apps and websites such as Purple Mash (where instructions are given on a class blog) and TT Rockstars; research activities may also be completed via the internet. In order to ensure children's safety and remind them how to keep safe online on a regular basis, an e-safety message is included at the start of every post in the year group blogs.

This message reiterate the rules for online safety. Children are told that should they ever feel unsafe, scared or worried whilst online they must inform an adult immediately. This will be a parent in the first instance but any concerns must also be reported to a member of school staff as soon as possible.

6.4 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or Disrupt teaching, and/or Break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police
-

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's Searching & Confiscation Policy
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

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.

8. Pupils using mobile devices in school

Pupils are not permitted to bring mobile devices into school.

Any breach of this rule by a pupil may trigger disciplinary action in line with the school behaviour policy and mobile phone policy, and will result in the confiscation of their device. A parent will then be required to collect the mobile device from the school office at the end of the day.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse of equipment or online abuse.

Where a pupil is found to be causing offence or harm to others through online abuse (including peer on peer abuse), we will follow the procedures set out in the behaviour policy. Further action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. The welfare of the victim will always be

paramount and incidents may involve the referral to M.A.S.H or the police depending on their severity.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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 (including peer on peer abuse) 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).

The DSL and the DDSLs 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 & DDSLs log behaviour and safeguarding issues related to online safety.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Mobile Phone Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Searching & Confiscation Policy
-

14. Monitoring and review

A summary of this policy will be shared with parents annually and the whole staff.
The Assistant Headteacher, Deputy Headteacher, Headteacher and the Governing Body will review the policy annually.

Reviewed and agreed by Governors:

Chair of Governors _____

Date_____