

# Online Safety Policy (E Safety)



**Approved by:** Penny Harris (Director) Jane Cox (Director) Steven Pryer (IT Manager) **Date:** 1 October 2022

**Last reviewed on:** 24<sup>th</sup> November 2022

**Next review due by:** 30 September 2023

All policies are generated and reviewed with an awareness of equality and diversity in relation to pupils, staff and visitors. All policies are generated placing safeguarding and wellbeing at the heart of all that we do.

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and directors
- 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, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## 2. Legislation and guidance

This policy is based on the 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 head teachers and school staff
- Relationships and sex education;
- 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.

### **3. Roles and responsibilities**

#### **3.1 The directorial board**

The directorial board has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation. The directorial board will co-ordinate regular meetings with appropriate staff to discuss online safety, and will monitor online safety logs.

The directors will:

- Ensure that 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 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 Head Teacher**

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The head teacher will also ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

#### **3.3 The E-Safety lead**

The E-Safety lead takes lead responsibility for online safety in school, in particular:

- Supporting the head teacher and senior leadership team to ensure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with 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
- Managing online safety issues in line with the school child protection 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 (appendix 3 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 head teacher and/or directorial board

This list is not intended to be exhaustive.

### **3.4 The IT manager**

The IT manager 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 on a termly basis.
- 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 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that online safety incidents and cyber-bullying incidents are dealt with appropriately
- Working with the E-Safety Lead to ensure that any online safety incidents are logged and dealt with appropriately in line with this 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**

Parents are expected to:

- Notify a member of staff or the head teacher 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 (appendix 1)

Parents 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 factsheet - [Childnet International](#)
- Healthy relationships - [Disrespect Nobody](#)

### **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 2).

## **4. Educating pupils about online safety**

Pupils will be taught about online safety as part of the curriculum. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Pupils at Key Stage 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 Key Stage 2, 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

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use group work opportunities to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. 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 about online safety**

The school will raise parents' awareness of internet safety in direct communications and via information on our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the E-Safety lead.

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

### **6. Remote Learning**

#### **a. Responsibilities:**

The directors are responsible for monitoring the school's approach to providing remote learning to ensure education remains as high quality and safe as possible. The SLT and subject leads are responsible for considering whether any aspects of the subject curriculum need to change to accommodate remote learning. SLT and subject leads are

responsible for working with teachers who are teaching remotely to ensure all work set is appropriate and consistent. SLT and subject leads are responsible for monitoring the remote work set by teachers. Teachers are responsible for continuing to set work for each pupil they are timetabled to teach. Teachers must be available on Google Classroom for the duration of each timetabled lesson. Teachers must provide feedback to pupils during each timetabled session. Teachers must record all attendance in lessons on Google Classroom. Teachers must record all communication with parents on a contact form. Teachers must record any concerns on a concern form. Communication with pupils and parents must only take place during school hours. The Designated Safeguarding Lead is responsible for child protection and wider safeguarding in relation to remote learning

#### **b. IT Issues and Safeguarding**

A staff member is allocated to help staff, parents and pupils with any technical issues they are experiencing during remote learning. Teachers will only use school equipment to deliver remote learning and not share these devices with family or friends.

### **7. Cyber-bullying**

#### **7.1 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. (See also the school behaviour policy.)

#### **7.2 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.

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, directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 12 for more detail).

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

#### **7.3 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

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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](#)
- The school's COVID-19 risk assessment

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

### **8. Acceptable use of the internet in school**

All pupils, parents, staff, volunteers and directors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 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.

We will monitor the websites visited by pupils, staff, volunteers, directors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

### **9. Pupils using mobile devices in school**

Pupils may bring mobile devices into school, but are not permitted to use them during lessons, without express permission from staff.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

### **10. 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, as set out in appendix 2.

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.

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

Work devices must be used solely for work activities. Work devices must not be shared with family or friends.

### **11. How the school will respond to issues of misuse**

Where a pupil misuses the school's ICT systems or internet, we will manage this in line with the school's behaviour management policy. Any action taken will depend on the individual pupil, 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

### **12. 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, 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 the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The E-safety lead will undertake child protection 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.

Directors 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.

### **13. Monitoring arrangements**

The DSL, head teacher and directors monitor incident logs and safeguarding issues related to online safety.

This policy will be reviewed annually by the directors and head teacher.

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour management policy
- Staff code of conduct policy
- Staff disciplinary policy
- Data protection and GDPR policy
- Complaints policy

## Appendix 1: 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 using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a staff member being present, or without a staff member's permission
- Access any inappropriate websites
- Access social networking sites (unless a staff member has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a member of staff
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of a staff member or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

#### When remote learning from home using live streaming, I will:

- Use appropriate language
- Wear appropriate clothing
- Behave appropriately
- Take care of school IT equipment
- Not record or take still photos of online lessons

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

- I will not use it during lessons without a staff member's permission
- 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.

I will immediately let a member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

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 for using personal electronic devices in school, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## **Appendix 2: acceptable use agreement (staff, directors, volunteers and visitors)**

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

**Name of staff member/director/volunteer/visitor:**

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which 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
- Share my password with others or log in to the school's network using someone else's details

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.

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) / E-Safety lead / head teacher 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.

**Signed (staff member/director/volunteer/visitor):**

**Date:**

### Appendix 3: online safety training needs – self-audit for staff

| Online safety training needs audit   |       |
|--|-------|
| Name of staff member/volunteer:  | Date: |
| Do you know the name of the person who has lead responsibility for online safety in school?                      |       |
| 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, directors and visitors?       |       |
| Are you familiar with the school's acceptable use agreement for pupils and parents?                              |       |
| 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? Please record them here. |       |

## Appendix 4: Online Safety Risks

We have to accept that we cannot completely monitor material held by pupils on mobile phones, tablets, etc, but we can ensure that sufficient information is given to students to allow them to make good decisions and help them to keep themselves safe. It is also the case that this is a very fast moving range of technologies and policies and procedures can be out of date almost as soon as they are written. We are also mindful that many students have greater knowledge than some staff in managing new technologies.

Broadly, online safety falls into three areas of risk:

**Content:** being exposed to illegal, inappropriate or harmful materials

**Contact:** being subjected to harmful online interaction with other users

**Conduct:** personal online behaviour that increases the likelihood of, or causes, harm

### Cyberbullying

Cyberbullying can take the following forms:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or video.
- 'trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding from online games, activities or friendship groups
- setting up hate sites or groups about a particular person
- encouraging to [self-harm](#)
- voting for or against someone in an abusive poll
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages
- sharing of nudes or semi-nudes

- pressuring into sending sexual images or engaging in sexual conversations.

**The sharing of nudes or semi-nudes** is when sexually explicit photos or messages are sent to other people's mobile phones. These photos/messages can then be forwarded and seen by many people, causing embarrassment and long term effects such as depression and anxiety.

It is a crime to send a sexually explicit photo to another person and under 18s can be charged with possessing and distributing child pornography. They can also be put on the sex offenders register.

The UKCCIS (UK Council for Child Internet Safety) Guidance: Sexting in schools and colleges, responding to incidents, and safeguarding young people (2017) will be followed by all staff.

### **Online grooming**

Grooming is when someone builds an emotional connection with a young person to gain their trust for the purposes of sexual abuse, exploitation or radicalisation. Groomers may be male or female and they could be of any age. Many young people do not understand that they have been groomed, or that what has happened has been abuse. Groomers can use social media sites, instant messaging apps or online gaming platforms to connect to a young person. They can spend time learning about a young person's interests from on-line profiles and then use this knowledge to help them build a relationship. It is easy for groomers to hide their identity on-line. They may pretend to be another young person and then chat and become 'friends' with the young person they are targeting.

Groomers may look for:

- Usernames that are flirtatious or have a sexual meaning
- Public comments that suggest a young person has low self-esteem or is vulnerable

Increasingly, groomers are sexually exploiting their victims by persuading them to take part in on-line sexual activity

### **Information and support**

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

[www.disrespectnobody.co.uk](http://www.disrespectnobody.co.uk)

[www.saferinternet.org.uk](http://www.saferinternet.org.uk)

[www.internetmatters.org](http://www.internetmatters.org)

[www.childnet.com/cyberbullying-guidance](http://www.childnet.com/cyberbullying-guidance)

[www.pshe-association.org.uk](http://www.pshe-association.org.uk)

[www.educateagainsthate.com](http://www.educateagainsthate.com)

[www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation](http://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation)