Sir Roger Manwood's School

Online Safety Policy

Date of Approval: November 2024

Date of Review: November 2026

Contents

1. Aims

Our school aims to:

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

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

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

It also refers to the DfE's guidance on protecting children from radicalisation.

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

This policy complies with our Funding Agreement and Articles of Association.

3. Links with other policies

This Online Safety Policy is linked to our:

- Safeguarding Policy
- Behaviour Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints Policy
- IT Acceptable Use Policy

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. It will ensure that:

- all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

- all staff receive regular online safety updates (e.g. by email, staff meetings, etc), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- regular meetings are held with appropriate staff to discuss online safety, requirements for training.
- monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).
- children are taught how to keep themselves and others safe, including keeping safe online.
- the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness including a review of the DfE filtering and monitoring standards, and discussing with IT staff and service providers 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.

All governors will:

- Ensure they have read and understood this policy
- Sign, and adhere to, the Acceptable Use Policy of the school's ICT systems and the internet
- Ensure that online safety is a running and inter-related theme while devising and implementing their whole-school approach to safeguarding and related policies and/or 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

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.

3.3 The Designated Safeguarding Lead (DSL) and their deputies

Details of the school's Designated Safeguarding Lead (DSL) and their deputies are set out in our Safeguarding Policy, as well as relevant job descriptions.

The DSL and their deputies take the lead responsibility for online safety in school, in particular:

- 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 and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT Manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's Safeguarding 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's Anti-Bullying and Behaviour Policies
- Updating and delivering staff training on online safety when required
- Liaising with other agencies and/or external services when required

- Providing regular reports on online safety in school to the Headteacher and/or Governing Body
- 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 intended to be exhaustive.

3.4 The IT Manager

The IT 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 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 IT 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 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 dealt with appropriately in line with the school's Anti-Bullying and Behaviour Policies

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 covered in the school's Acceptable Use Policy of the school's IT systems and internet, and ensuring that students follow those same terms too
- 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
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes e.g. requesting, via the DSL, the IT Manager to unblock the website they wish students to use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's Anti-Bullying and Behaviour Policies
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff, the relevant member of the pastoral staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the IT Acceptable Use Policy

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
- Kent Safeguarding Children Multi-Agency Partnership (KSCMP) – www.kscmp.org.uk

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or access the internet via the School's wifi or hard wired network will be made aware of this policy, when relevant, and are expected to read and follow it.

If appropriate, they will be expected to sign the IT Acceptable Use Policy before being able to do so.

4. Educating pupils about online safety

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

All schools have to teach:

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

In **KS3**, 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 **KS4** 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**, pupils 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 that 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 whenever it is relevant, especially in PSHCE (Personal, Social, Health and Careers Education) and also in tutorial time.

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

5. Educating parents/carers about online safety

This policy will be shared with parents and carers. In addition, the school will raise awareness of online safety amongst parents and carers via communications home and information evenings.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the relevant member of the pastoral staff (all of whom are Deputy DSLs) or the DSL.

Concerns or queries about this policy can be raised with the DSL or 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 intentional harming of 1 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. This will be covered primarily in PSHCE and Computer Science lessons, but Form Teachers will also discuss cyber-bullying with their tutor groups from time to time.

All staff and governors receive training on cyber-bullying as part of their safeguarding training (see section 11 for more detail).

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

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Anti-Bullying and Behaviour Policies. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

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

6.3 Examining electronic devices

The 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 DSL or one of their deputies if the DSL is unavailable
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL, or one of their deputies if the DSL is unavailable, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a

suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's Behaviour Policy

Any complaints about searching for, or deleting, inappropriate images or files on students' electronic devices will be dealt with through the Complaints Policy.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The 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 create images, audio or video hoaxes that look real.

The School will treat any use of AI to bully pupils in line with its Anti-bullying and Behaviour Policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment when new AI tools are being used in their classroom or are required to be used for specific pieces of homework.

7. Acceptable use of the internet in school

All students, parents/carers, staff and governors sign an agreement regarding the acceptable use of the school's IT systems and the internet. Volunteers and visitors will be expected to read and agree to the school's terms on acceptable use if they require access to the school's IT systems.

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.

The School restricts access from its IT systems and devices to websites through the action of a filtering system. It also monitors the sites visited by students, staff, governors and volunteers/visitors (where relevant) to ensure they comply with the IT Acceptable Use Policy.

8. Pupils using mobile devices in school

Any use of mobile devices in school by students must be in line with the Code of Conduct contained in the School's Policy on the use of mobile devices.

Any breach of the Code, is contained in the Student Planner and which students sign at the start of each year, may trigger disciplinary action in line with the school's Use of Mobile Devices Policy and Behaviour Policy. This may result in the confiscation of their device.

9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Ensuring that the anti-virus and anti-spyware software installed by the School's IT Support Technicians before they are given their School laptop remains active and is not deleted or otherwise changed from the original install
- Ensuring that the operating system installed on their School laptop, and kept up to date by the School IT Support Technicians, is not changed or in any way altered

Staff members must not use the device in any way that would violate the school's IT Acceptable Use Policy.

Work devices must be used solely for work activities.

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

10. How the school will respond to issues of misuse

Where a pupil misuses the School's IT systems or internet, the procedures set out in our policies on Behaviour and IT Acceptable Use will be followed. 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 IT systems or the internet, or misuses a personal or work device where the action constitutes misconduct, the matter will be dealt with in accordance with the relevant policy/policies e.g. IT Acceptable Use, Electronic Information and Communications Systems, Employee Code of Conduct, Social Media and Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

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

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

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

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

Volunteers will receive appropriate training and updates, if applicable.

12. Monitoring arrangements

The DSL and their deputies log behaviour and safeguarding issues related to online safety on CPOMS.