

ONLINE SAFETY POLICY



DOCUMENT STATUS

Version	Date	Action
Version 1	Oct 2021	New Policy agreed by Standards & Quality Committee
	Oct 2022	Reviewed by Standards & Quality Committee
	Dec 2023	Changes 3.1
Review Period	Annually	
Review Date	Dec 2024	September 2027
	September 2026	Updated to reflect KCSIE 2026 and current DfE online safety, filtering and monitoring, AI, RSE and data protection guidance

Contents

1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	5
5. Educating parents about online safety	6
6. Cyber-bullying	6
7. Acceptable use of the internet in school.....	8
8. Pupils using mobile devices in school	8
9. Staff using work devices outside school.....	8
10. How the school will respond to issues of misuse.....	9
11. Training.....	9
12. Monitoring arrangements	10
13. Links with other policies	10
Appendix 1: online safety training needs – self audit for staff	10
Appendix 2: online safety incident report log.....	12

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, 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, including pornography, child sexual abuse material, racism, misogyny, self-harm and suicide content, misinformation and disinformation, harmful or misleading AI-generated content and deepfakes, and material linked to radicalisation and extremism.
- Contact – being subjected to harmful online interaction with other users, including peer pressure, bullying or harassment, commercial contact, scams, and adults or others seeking to groom, exploit or coerce children for sexual, criminal, financial or other purposes.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, including bullying or harassment, making, requesting, sending or receiving sexual images, consensual and non-consensual sharing of nudes and semi-nudes, sexualised or misogynistic behaviour, impersonation, misuse of AI and sharing harmful or abusive content.
- Commerce – risks such as online gambling, inappropriate advertising, phishing, fraud, financial scams and other commercial exploitation.

2. Legislation and guidance

This policy is based on the Department for Education (DfE) statutory safeguarding guidance Keeping Children Safe in Education 2026 (KCSIE), in force from 1 September 2026, and should be read alongside the school's Child Protection and Safeguarding Policy.

- DfE guidance on Teaching online safety in schools and the National Curriculum computing programmes of study
- DfE guidance on Preventing and tackling bullying and cyber-bullying
- DfE statutory guidance on Relationships Education, Relationships and Sex Education (RSE) and Health Education, revised from 1 September 2026
- DfE guidance on Searching, screening and confiscation

It also has regard to the Prevent duty guidance, DfE Filtering and Monitoring core standard, Cyber Security core standard, Generative artificial intelligence (AI) in education guidance, Generative AI product safety standards, and DfE Data protection in schools guidance.

The school recognises that online safety is an integral part of safeguarding. Technology can facilitate abuse and exploitation, and safeguarding arrangements therefore apply to school systems, devices, online services, remote access and the use of emerging technologies, including generative AI.

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 safeguarding, including online safety, and for ensuring that appropriate filtering and monitoring systems are in place. It will hold the headteacher to account for implementation of this policy and KCSIE 2026 requirements.

The governing body will receive appropriate information and assurance about online safety, filtering and monitoring, cyber security and emerging risks, including generative AI.

The governing body will ensure that filtering and monitoring provision is reviewed at least annually, that roles and responsibilities are clearly assigned, and that the school's systems block harmful and inappropriate content without unreasonably affecting teaching and learning.

Link governor responsible: Mrs Fiona Roper (Safeguarding Link Governor)

All governors will:

- Ensure that they have read and understand this policy and receive appropriate safeguarding and online safety training, including their responsibilities for filtering and monitoring
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet ([ICT & Internet Acceptable Use Policy](#))
- 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 headteacher

The headteacher is responsible for ensuring that staff understand this policy and that it is implemented consistently, including ensuring appropriate resources, training and oversight for online safety, filtering and monitoring and cyber security.

The headteacher will work with the DSL, ICT manager/technical provider and governing body to ensure that safeguarding and technical responsibilities are joined up and that identified risks are acted upon promptly.

3.3 The designated safeguarding lead

Details of the school's DSL and Deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place in school. In particular, the DSL is responsible for:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with SLT, ICT staff/technical providers and other staff to address online safety issues, filtering and monitoring concerns, emerging technologies and safeguarding risks
- Receiving and responding to safeguarding alerts or concerns arising from monitoring systems, ensuring that technical alerts are interpreted in the context of the child and recorded or escalated where appropriate.
- Ensuring online safety risks, including risks associated with generative AI, are reflected in safeguarding practice, staff training and the school's annual risk assessment.
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 2) 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 (appendix 1 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 governing body (Mrs Fiona Roper Safeguarding Link Governor)
- This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager, supported by the school's technical provider, is responsible for:

- Maintaining appropriate filtering and monitoring systems in line with KCSIE and the DfE Filtering and Monitoring core standard, including coverage of school-managed devices and services and consideration of generative AI risks.
- Ensuring that the school's ICT systems are secure, appropriately configured and maintained in line with the DfE Cyber Security core standard, with security updates, malware protection, access controls, backups and other safeguards kept under review.
- Supporting an annual documented review of filtering and monitoring provision, and more frequent checks where risks, systems or providers change, with outcomes reported to the headteacher, DSL and governing body.

- Ensuring changes to filtering and monitoring settings are authorised, recorded and tested, and that safeguarding concerns or technical failures are escalated promptly to the DSL and headteacher.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Liaising with headteacher and link governor to implement and quality assure security protection procedures

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:

- Reading KCSIE 2026 Part One in full, understanding this policy and knowing the school's procedures for reporting safeguarding and online safety concerns
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet ([Internet & Acceptable Use Policy](#) appendix 4), and ensuring that pupils follow the school's terms on acceptable use (appendices 2 and 3)
- Reporting online safety incidents, harmful content, suspected abuse, filtering or monitoring concerns and attempts to bypass school controls promptly to the DSL in accordance with safeguarding procedures
- Staff must not investigate safeguarding concerns themselves or view, copy, forward, save or share sexual images of children except where specifically required by statutory guidance and directed by the DSL. Incidents involving sharing nudes or semi-nudes will be managed in line with current UKCIS guidance.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers 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](#)

- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)
- National Online Safety

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:

The text below is taken from the [National Curriculum computing programmes of study](#).

It also reflects the revised DfE statutory guidance on Relationships Education, Relationships and Sex Education (RSE) and Health Education in force from 1 September 2026.

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

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 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
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Online safety will be taught in an age-appropriate, sequenced way across the curriculum. Teaching will include safe and respectful behaviour, privacy and personal data, reporting concerns, healthy boundaries, misinformation and disinformation, scams and manipulation, harmful content, online sexual harassment, sharing nudes and semi-nudes where age appropriate, and the safe and responsible use of emerging technologies including generative AI.

Pupils will be taught that AI-generated information may be inaccurate, biased or fabricated; that images, audio and video can be manipulated; and that they should not enter personal, sensitive or confidential information into AI tools. Any pupil use of generative AI in school will be age-appropriate, supervised and limited to tools approved by the school.

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

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

Online safety will also be covered during parents' evenings and useful information/signposting will be shared in the parents' section of our website and as a regular information section within our newsletter.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL or Deputies.

Concerns or queries about this policy can be raised with any member of staff or 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. (See also the school behaviour for learning policy.)

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.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also shares information on cyber-bullying with parents via school website and within our school newsletter so that 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 school Behaviour for Learning & Anti-Bullying 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 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.

6.3 Examining electronic devices

Searching, screening and confiscation will be carried out only in accordance with current DfE guidance and the school's Behaviour and Safeguarding policies. Staff should involve the DSL where a search may reveal a safeguarding concern or sexual imagery.

Where there is a lawful basis to examine data or files on a device, staff will act proportionately, protect the child's welfare and preserve evidence where a criminal or safeguarding matter may be involved. Staff must not routinely view, copy, print, share, save or delete nude or semi-nude images of children; the DSL will follow current UKCIS guidance and seek police or specialist advice where required.

- Any search or examination must have a clear safeguarding, disciplinary or legal basis and be recorded appropriately.
- The least intrusive appropriate action will be used, with due regard to the pupil's age, needs and circumstances.
- Where there is uncertainty about illegal content or preservation of evidence, staff will not delete material and will seek advice through the DSL.
- If inappropriate or illegal material is found or suspected, the DSL or senior leader will decide the appropriate safeguarding response, including whether external agencies or the police should be involved.
- Any decision to delete material will be made only where lawful and consistent with DfE/UKCIS guidance and will be recorded.
- Potential evidence of a criminal offence or abuse will be preserved and handled in accordance with police or safeguarding advice.
- The school will report matters to the police or other agencies where required or appropriate.
- 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

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

All pupils, parents, staff, volunteers and governors are expected to adhere to an agreement regarding the acceptable use of the school's ICT systems and the internet (see [ICT & Internet Acceptable Use Policy](#)). 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.

Use of school systems and devices may be filtered and monitored for safeguarding, security and acceptable-use purposes. Monitoring will be proportionate, transparent and handled in accordance with safeguarding and data protection requirements. Pupils and staff will be informed that school systems are subject to filtering and monitoring.

More information is set out in the acceptable use policy

8. Pupils using mobile devices in school

Pupils in Years 5 or 6 who have written permission to travel to and from school independently may bring a mobile phone to school in accordance with the school's Use of Mobile Phones Policy. The same principles apply to smart watches and other personal connected devices unless the school has agreed a reasonable adjustment or specific exception.

Pupils must ensure mobile phones are turned off as they enter the school gate.

All pupil mobile phones must be handed in at the beginning of the school day and stored in a designated area.

Mobile phones must not be accessed or switched on at any point during the school day.

Pupils must not turn their mobile phone back on until they are leaving the school premises.

Under no circumstances, should mobile phones be kept in pupils' lockers, bags or pockets after arrival in the classroom.

Pupils are not authorised to take mobile phones on school trips or residential visits.

If any pupil breaches these arrangements, their mobile phone will be confiscated by a teacher and stored in the school office until it can be collected by their parent/carer.

Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the **Education and Inspections Act 2006**)

Any confiscation, search or examination of a pupil's device will be carried out in accordance with current DfE Searching, screening and confiscation guidance and the safeguards set out in section 6.3 of this policy.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies as appropriate. Such conduct includes, but is not limited to:

Sharing of Nudes or Semi-Nudes

Threats of violence or assault

Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation

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:

- Using strong, unique authentication in accordance with the school's current technical security requirements, including multi-factor authentication where provided; passwords and authentication details must never be shared
- 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
- Installing anti-virus and anti-spyware software (managed by Hi-Impact)
- Keeping operating systems up to date – always install the latest updates (managed by Hi-Impact)

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns about the security of a device, account or data, or believe a device has been lost, stolen, compromised or subject to phishing or malware, they must report this immediately to the school and technical support so that safeguarding, cyber security and data breach procedures can be followed.

Staff must not enter pupil personal data, safeguarding information or other confidential school information into public or unapproved generative AI tools. Only school-approved AI services may be used for school business, in accordance with data protection, safeguarding, copyright and acceptable-use requirements.

10. 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 for learning & anti-bullying and ICT and internet acceptable use. 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 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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents involving illegal activity or content, child sexual abuse material, sexual imagery, threats, exploitation, fraud, radicalisation or other serious harm should be referred to the police, children's social care or another appropriate agency. Safeguarding concerns will be managed through the DSL and the school's child protection procedures.

11. Training

All new staff members will receive safeguarding training as part of induction, including online safety, the school's filtering and monitoring arrangements, cyber-bullying, online sexual harassment, radicalisation, data security and relevant risks from generative AI.

All staff will read KCSIE 2026 Part One in full and receive safeguarding and online safety training at induction and regularly thereafter, with at least annual updates and additional updates when risks, guidance or school systems change.

Training will ensure staff understand their role in filtering and monitoring, how to report concerns or system failures, and that technical controls do not replace professional curiosity, supervision or safeguarding practice.

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 DSL and deputies 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 appropriate safeguarding and online safety training, including their strategic responsibilities for filtering and monitoring. They will ensure that KCSIE requirements are

understood and that the school receives appropriate assurance about the effectiveness of its arrangements.

Volunteers will receive appropriate training and updates, as applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL will ensure safeguarding concerns related to online safety are recorded in the school's safeguarding system. Technical alerts and filtering/monitoring incidents will be reviewed and escalated in line with agreed roles and procedures; Appendix 2 may be used for non-safeguarding online safety incidents where appropriate.

This policy will be reviewed at least annually by the headteacher and shared with the governing body Standards & Quality Committee. The review will be informed by KCSIE, current DfE guidance, incident data, pupil needs, technology changes and an annual assessment of the online risks pupils face.

Filtering and monitoring provision will be reviewed at least annually, and sooner following a significant incident or material change to systems or risk. The review will consider roles and responsibilities, risk profiles, blocked content, monitoring effectiveness, safeguarding response arrangements, generative AI and whether controls support teaching and learning without creating avoidable risk.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour for learning & anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Use of mobile phones and smart devices policy
- Generative AI / acceptable use guidance (where adopted)

Appendix 1: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
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, governors 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?	

Appendix 2: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident