Online Safety Policy

PERSON RESPONSIBLE FOR POLICY:	**D. DUKES**
REVIEWED:	**DATE: NOVEMBER 2026**
TO BE REVIEWED:	**2 YEARS**

1. Aims

2. Legislation and guidance

3. Roles and responsibilities

4. Educating pupils about online safety

5. Educating parents/carers about online safety

6. Cyber-bullying

7. Acceptable use of the internet in school

8. Pupils using mobile devices in school

9. Staff using work devices outside school

10. How the school will respond to issues of misuse

11. Training

12. Monitoring arrangements

13. Links with other policies

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)

Appendix 4: Online safety training needs – self audit for staff

Appendix 5: Online safety incident report log

1. Aims

Our school aims to:

This policy applies to school-managed systems and devices, approved online learning, relevant use of personal devices and online behaviour affecting the school community, including incidents outside school. Teaching and support will reflect pupils' actual ages, developmental stages and needs.

- 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, 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 (DfE) statutory guidance Keeping Children Safe in Education 2026 (KCSIE). It is read alongside the statutory Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance effective from 1 September 2026, Mobile phones in schools statutory guidance, and Prevent duty guidance: England and Wales (2023). Schools must have regard to applicable statutory guidance. Supporting non-statutory advice includes:

Teaching online safety in schools•

• Preventing and tackling bullying and advice on cyberbullying for school staff

• Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS, updated March 2024)

Searching, screening and confiscation•

The DfE filtering and monitoring and cyber security standards provide practical guidance on meeting safeguarding expectations. Relevant official sources are listed at the end of this section.

The policy reflects applicable legislation, including the Education Act 2002, Education Act 1996 (including search powers), Education and Inspections Act 2006, Equality Act 2010, Data Protection Act 2018, UK GDPR and applicable amendments under the Data (Use and Access) Act 2025. Applicable school standards and safeguarding duties depend on the school's legal status. Searching, confiscation and examination or deletion of files are separate powers with safeguards; section 6.3 sets out the school's approach.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will make sure 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.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board has strategic oversight of appropriate filtering and monitoring on school devices and networks. It will designate a responsible senior leader and governor, obtain assurance that provision is effective and review the DfE standards with the DSL and IT support. The arrangements will include:

- Identifying and recording the responsibilities of the senior leader, responsible governor, DSL, IT support and any external provider;

- Reviewing effectiveness at least once every academic year, recording checks, findings and actions;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The responsible senior leader will lead the annual effectiveness review, supported by the DSL and IT support and involving the responsible governor. Checks will cover internet-connected devices, user profiles and relevant locations, including off-site use of school-managed devices where applicable. Results, limitations, exceptions, actions, owners and completion dates will be recorded. Checks will also follow significant system or equipment changes.

The school will record how alerts are prioritised, who reviews them, response arrangements during operating hours and cover for absence. Urgent safeguarding alerts must be escalated immediately to the DSL or deputy. Staff, pupils and parents will be told the limits of monitoring, including arrangements outside school hours; monitoring must not be presented as a continuously staffed emergency service.

All governors will:

- Ensure 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 3)
- Ensure that online safety is a running and interrelated 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 principal

The principal is responsible for ensuring staff understand this policy and that it is implemented consistently. The principal will identify a senior leader responsible for filtering and monitoring and ensure that responsibilities, cover and escalation routes are recorded and communicated. Strategic oversight and safeguarding decisions remain with the school when technical services are outsourced.

3.3 The designated safeguarding lead

Details of the DSL and deputy DSLs, including how to contact them and cover arrangements, are set out in the child protection and safeguarding policy. The DSL

has lead responsibility for online safety, including understanding the school's filtering and monitoring systems and processes; this responsibility must be explicit in the DSL's job description. Any E-Safety Lead supports the DSL and does not replace the DSL's safeguarding accountability.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) 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 4 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 principal and/or governing board
- • Checking relevant monitoring reports, assessing and responding to safeguarding alerts, ensuring appropriate cover and referrals, and contributing to recorded reviews and assurance for governors

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Implementing and maintaining the filtering and monitoring systems agreed by senior leaders, working with the DSL and providing technical advice, reports and prompt action on identified weaknesses
- 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (see appendix 5) 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 behaviour policy

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 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'
- Recognising that filtering is not a substitute for supervision or safeguarding action; promptly reporting harmful content, failed blocks, inappropriate restrictions, bypass attempts and concerns about monitoring to the DSL and IT support

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the principal 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 (appendices 1 and 2)

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

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 3).

4. Educating pupils about online safety

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

Online safety teaching will follow the applicable statutory Relationships Education, RSE and Health Education guidance effective from 1 September 2026, with a planned, age-appropriate progression across the school's actual phases:

- Relationships Education and Health Education for primary pupils, with relevant computing curriculum requirements also addressed.

Online safety is integrated into this teaching and revisited as risks and pupils' needs change. The following primary outcomes are supplemented by the wider RSHE curriculum, including internet safety and harms.

This new requirement includes aspects about online safety.
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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- How to resist pressure to share personal information or images and respect other people's boundaries.
- • How privacy and location settings can protect information, and why sharing information requires caution.
- • That online words and pictures can be copied and circulated beyond their control and cannot reliably be deleted everywhere.
- • That social media services have age restrictions; pupils will learn why these exist and how to check the rules for a service.
- • How to seek help with upsetting content or contact and keep asking until they are heard; abuse is never the child's fault.
-

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

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

The school will use Team meetings to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Approved online learning will use school-authorised accounts, platforms and communication channels. Staff will maintain professional boundaries in live sessions and messaging, apply school rules on recording and images, and tell pupils and parents how to report concerns. Parents will be told which sites and tools pupils are expected to use and who will communicate with them.

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 with parents/carers.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- How to report concerns, including outside school hours; relevant changes in online risks and practical support on privacy, gaming, social media, image sharing and AI.

Parents/carers should raise online safety concerns with a member of staff, the principal or the DSL. Staff will refer safeguarding concerns promptly to the DSL or deputy. Any E-Safety Lead works under the DSL's safeguarding oversight.

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

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place through technologies such as social media, messaging and gaming. Like other bullying, it involves intentional harm, repetition and an imbalance of power. A single upload may cause repeated harm through sharing or continued access. Staff will respond to every harmful online incident, including a one-off incident, without waiting for repetition or a bullying label. See also the behaviour and child protection and safeguarding policies.

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 team groups, and the issue will be addressed in assemblies.

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 sends information/leaflets on cyber-bullying to parents 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 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 assess safeguarding needs and follow the child protection and safeguarding policy and applicable referral guidance. Where possession of material is suspected to be illegal, staff will preserve the device and seek police advice promptly; they must not forward or copy suspected indecent images of children. Devices or evidence will be handed to police as required by the searching guidance. Support and protection for the child will not wait for a criminal investigation.

6.3 Examining electronic devices

The principal, or staff authorised by the principal, may search a pupil or their possessions without consent only where the relevant legal grounds are met: reasonable grounds to suspect a prohibited item under legislation, or an item identified in school rules as one for which a search may be made. A general concern that a device poses a risk does not itself create an unrestricted search power. Searches and confiscation are separate decisions. An authorised member of staff carrying out a lawful search may confiscate an item they reasonably suspect:

- Poses a risk to staff or pupils, and/or
- Is prohibited or is identified in school rules as an item for which a search may be made, and/or
- Is evidence in relation to an offence

Before a search, the authorised member of staff must establish the lawful search grounds described above and will also:

- Assess urgency, safeguarding risks, the pupil's needs and any reasonable adjustments; seek advice from the principal, authorised deputy or DSL where safe and practicable
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Searches will follow the full DfE safeguards, including the normal same-sex searcher and witness requirements and their limited urgent exceptions, privacy, dignity and additional safeguarding needs. Staff may require removal of outer clothing only; school staff must not conduct strip searches. The searching guidance and behaviour policy govern records and informing parents; searches for statutory prohibited items and searches by police must be recorded, and parents informed as soon as practicable as required by the guidance. Safeguarding concerns must be reported to the DSL promptly.

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, staff will refer safeguarding concerns immediately to the DSL or deputy and take protective action. The principal or authorised deputy will decide any disciplinary response in consultation with the DSL where safeguarding is involved. Evidence of a suspected offence must be preserved and handled in accordance with the DfE searching guidance and police advice.

When deciding whether there is good reason to erase files, staff must first consider whether the material may be evidence of a suspected offence. Such material must not be deleted and the device must be handed to police as soon as reasonably practicable. Where files are not suspected evidence of an offence, staff may delete them only when both of the following conditions apply:

- Their continued existence is likely to continue to cause harm to a person; and
- The pupil and/or parent refuses to delete the files themselves.
- If staff suspect a device contains an indecent image of a child, including a digitally manipulated or AI-generated image, they will:
- Not intentionally view the image, or copy, print, forward, share, store or save it; not ask a pupil to send or show it to them
- Secure or confiscate the device where lawful, avoid examining its contents and refer immediately to the DSL or deputy. The DSL will follow KCSIE, the DfE Searching, screening and confiscation guidance and UKCIS Sharing nudes and semi-nudes advice. Any exceptional decision about viewing must meet the UKCIS safeguards and be recorded; routine investigation by staff is not permitted.

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
- Our behaviour policy

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

6.4 Sharing nudes and semi-nudes and sexual extortion

Reports involving sexual images, including manipulated or AI-generated images, coercion, grooming or demands for money must be referred immediately to the DSL or deputy. Staff will listen calmly, reassure the child that seeking help is right, avoid blame and not promise secrecy or conduct their own investigation. They must not ask the child to download, forward or recreate imagery.

The DSL will carry out an initial review and risk assessment under UKCIS advice, consider whether an adult may be involved even if an account appears to belong to a child, and arrange immediate safety and emotional support. Decisions on referrals to children's social care or police, involving parents, device handling and image removal support will follow the guidance and be recorded with reasons. Parents will normally be involved unless doing so would put the child at risk; the DSL will seek agency advice where needed.

In sexual extortion cases the child should be supported not to pay or send further images and to obtain urgent specialist or police support. Evidence will be preserved safely without copying illegal images. The DSL will consider appropriate removal and reporting services, including Report Remove or Take It Down where suitable, without asking the child to obtain another copy. Support will continue for affected children, including those alleged to have caused harm.

.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

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

More information is set out in the acceptable use agreements in appendices 1, 2 & 3. Only school-approved digital services, apps and AI tools may be used for school activities. Senior leaders will consult the DSL, IT support and data protection officer as appropriate before approval, assess age restrictions, privacy, safeguarding, accessibility and filtering/monitoring limitations, and record the decision. Unapproved tools must not receive personal, confidential or safeguarding information. AI output requires human checking and must not be relied on for safeguarding decisions.

Reviews will consider real-time, personalised and AI-generated content, including embedded AI in browsers and apps, and relevant DfE generative AI product safety standards. Known gaps will be mitigated or access restricted. Pupils must not bypass controls, create abusive deepfakes, impersonate others or use AI to facilitate bullying or exploitation.

Filtering and monitoring will be proportionate and explained in appropriate privacy information, including what is collected, purposes, access and retention. The data protection officer will advise on lawful processing, provider arrangements and any

required impact assessment. Monitoring notices and acceptable use signatures do not replace the school's need for a lawful basis.

8. Pupils using mobile devices in school

The school is a mobile phone-free environment by default. Pupils must not access or use mobile phones or smart technology with similar communication or recording functions throughout the school day, including:

- Lessons and the time between lessons
- Team time, breaktimes and lunchtime
- School clubs and activities before or after school, subject to the specific arrangements for trips and individual adaptations below

The restriction covers relevant smartwatches and other connected communication or recording devices. School-approved laptops or tablets used for learning are governed by the school's ICT acceptable use arrangements; mobile phones are not part of a learning BYOD scheme.

Pupils bringing a mobile phone or relevant smart device to school must hand it to their Team Teacher at the start of the day and collect it at the end. Devices will be stored securely under the school's agreed custody arrangements. Parents/carers should contact the school office for urgent messages rather than contacting pupils directly during the school day.

Individual adaptations will be assessed and recorded for disability, medical needs and other justified circumstances, including young carers. The school will make reasonable adjustments and support medical needs, for example phone-linked glucose monitoring. Agreements will specify purpose, times, locations and review. Pupils may access a device with staff support when necessary to report an online concern.

The principal will set and communicate phone arrangements for trips and residential activities, balancing education, welfare and family contact. Staff will model the rules and avoid personal phone use in front of pupils, apart from authorised professional or necessary individual uses.

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.

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 unique, strong passwords or passphrases that meet the school's IT-managed security standard, for example machine-generated passwords or three random words; using approved password managers where provided and changing any compromised or suspected compromised password immediately
- 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
- Using school-approved, centrally managed malware protection; staff must not install unapproved security software
- Allowing IT support to apply operating system, application and security updates promptly and not disabling security controls
- Using multi-factor authentication for staff accounts accessing cloud services or remote access to on-site systems, and for IT administrator accounts; IT support will provide approved alternatives or accessibility support where needed
- Using only approved secure storage, remote access and transfer methods; maintaining school-managed backups and not transferring work data to personal accounts, storage or unapproved removable media

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

Staff must report a lost or stolen device, suspected phishing, compromised account, malware or data breach to IT support and the principal immediately through the school's incident route, and inform the DSL promptly where a child may be at risk. The data protection officer will be involved where personal data is affected. Staff must not delay reporting while attempting their own investigation.

10. How the school will respond to issues of misuse

Where a pupil misuses ICT or the internet, staff will first consider safeguarding needs, including exploitation, grooming, child-on-child abuse and harmful sexual behaviour. Concerns must be referred promptly to the DSL or deputy and managed through the child protection and safeguarding policy alongside any proportionate behaviour response. The school will address relevant incidents outside school where they affect pupils' safety or the school community.

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

Online concerns about staff, including conduct on personal devices or outside work, must be reported through the child protection and safeguarding policy's staff allegation or low-level concern procedures as appropriate. Concerns about the principal go to the chair of governors or the alternative person specified in that policy. The principal or appropriate case manager will seek local authority designated officer (LADO) advice where the harm threshold may be met. Staff disciplinary action will follow the relevant procedure alongside safeguarding action.

The DSL or appropriate case manager will make referrals to children's social care and/or police when required under safeguarding procedures and local thresholds, recording decisions and reasons. Anyone may make a safeguarding referral where necessary. Immediate danger requires emergency action; staff must not wait for the DSL's availability.

11. Training

All new staff will receive safeguarding induction covering online safety, cyber-bullying, radicalisation, child-on-child abuse, AI-related risks and their specific filtering and monitoring responsibilities, including alert handling and escalation. All staff must read KCSIE 2026 Part one and be helped to understand and apply it.

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 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 deputy DSLs will undertake safeguarding and child protection training at least every two years, including online safety, and update knowledge and skills regularly and at least annually. Their training will include the filtering and monitoring systems and processes in use and relevant Prevent awareness. The principal and other senior leaders will receive training appropriate to their safeguarding and oversight roles.

Governors will receive safeguarding and child protection training, including online safety, at induction and regularly thereafter. The responsible governor and senior leader will understand the assurance needed on filtering, monitoring and cyber security.

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 will ensure online safeguarding concerns, decisions, reasons, referrals, support and follow-up are recorded securely in the school's approved safeguarding recording system. Appendix 5 provides a recording template or checklist; it must not become an unsecured parallel record or include illegal imagery. Access, retention and information sharing will follow safeguarding and data protection procedures.

The principal and DSL will review this policy and the school's online safety approach at least annually, supported by an annual risk assessment reflecting pupils' ages, vulnerabilities, SEND, technology use and emerging harms. The governing board will consider and approve the review. Earlier review will follow significant incidents or changes to guidance, technology or provision. The filtering and monitoring review will also take place at least once every academic year, with recorded checks, findings, actions and completion dates.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy
- Complaints procedure

Appendix 1: EYFS and KS1 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 I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them.
- Only use websites that a teacher or adult has told me or allowed me to use.

Tell my teacher immediately if:

- I click on a website by mistake.
- I receive messages from people I don't know.
- I find anything that may upset or harm me or my friends.
- Use school computers for school work only.
- I will be kind to others and not upset or be rude to them.
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly.
- Only use the username and password I have been given.
- Try my hardest to remember my username and password.
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer.
- Save my work on the school network.
- Check with my teacher before I print anything.
- Log off or shut down a computer when I have finished using it.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

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: KS2, KS3 and KS4 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:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only.
- Only use them when a teacher is present, or with a teacher's permission.
- Keep my username and passwords safe and not share these with others.
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer.
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others.
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Use any inappropriate language when communicating online, including in emails.
- Log in to the school's network using someone else's details.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

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

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher'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 and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's 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 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- 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, or connect unauthorised hardware or devices to the school's network.
- Share my password with others or log in to the school's network using someone else's details.
- Take photographs of pupils without checking with teachers first.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote private businesses, unless that business is directly related to the school.

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 and my use of the school's ICT facilities and systems.

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) and ICT manager 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/governor/volunteer/visitor):

Date:

Appendix 4: 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?

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 5: 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