Mill Lodge Primary School
Online safety policy

Approved by: Behaviour, Health and Safety Committee		**Date:** 21/05/26
Last reviewed on: New version		
Next review due by:	Summer 2027	

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Contents

1. Aims 2
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 7
5. Educating parents/carers about online safety 8
6. Cyber-bullying 8
7. Acceptable use of the internet in school 11
8. Pupils using mobile devices in school 11
9. Staff using work devices outside school 11
10. How the school will respond to issues of misuse 12
11. Training 13
12. Monitoring arrangements 15
13. Links with other policies 15
Appendix 1: EYFS and KS1 acceptable use agreement (pupils) 17
Appendix 2: KS2 (pupils) 18
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 19
Appendix 4: online safety training needs – self-audit for staff 20

1. Aims

Online safety is embedded within the school's whole-school safeguarding approach. The school recognises that online safety is not a standalone issue, but is integral to safeguarding and child protection. All staff understand that online risks can manifest in many areas of a child's life and that concerns should always be considered within the wider safeguarding context.

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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- **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 the user 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 (RSE) and health 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.

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

This policy also reflects the Department for Education's filtering and monitoring standards and the UK Council for Internet Safety (UKCIS) *Education for a Connected World* framework. It takes into account the need for schools to have effective systems in place to safeguard pupils from online harm, including through appropriate filtering, monitoring and staff response.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher 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 and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the 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 the school's safeguarding needs

The governor who oversees online safety is **Gareth Harries**.

All governors will:

- Make sure 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)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure 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 making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and make sure 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
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the local authority to make sure the appropriate systems and processes are in place
- Working with the local authority 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 child protection policy
- Escalating serious concerns for online harms (such as online grooming, radicalisation/ extremism, sexual exploitation or nude/ semi-nude image sharing) in line with the school's safeguarding and child protection policy
- Ensuring staff know and understand the school's data protection policy and operate within the parameters set out by this

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- 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 headteacher with the local authority

The headteacher and local authority are responsible for:

- Putting in place and maintaining 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 make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- The headteacher will review alerts that are received from the filtering and monitoring service daily, and escalate when necessary
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged through CPOMs and dealt with appropriately in line with this policy
- Categorise and analyse all online safety concerns reported
- Regularly review patterns and trends and use these findings to inform risk assessments and curriculum planning
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Approval and risk assessment of and new apps or digital platforms

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

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 by logging the incident
- Following the correct procedures by making a request to the headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure 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'
- Ensure they adhere to the school's social media policy
- Ensure they adhere to the school's data protection policy
- Maintain professional boundaries when communicating online and only use school-approved systems
- Not use personal devices or accounts to contact pupils
- Ensure that any online activity involving pupils is transparent and appropriate

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
- Make sure that 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/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

3.8 Filtering and monitoring (operational detail)

The school uses appropriate filtering and monitoring systems to safeguard pupils and staff when using school devices and networks.

The school currently uses:

- Filtering system: Internet content is filtered by the local authority and school liaise with LA to ensure this remains robust.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Monitoring system: Smoothwall

These systems are designed to:

- Block access to inappropriate and harmful content
- Identify potential safeguarding concerns through monitoring alerts
- Support staff in responding to online safety risks

Roles and responsibilities:

- The DSL has overall responsibility for managing filtering and monitoring
- The headteacher manages the day-to-day operation of systems
- Alerts are reviewed daily by the headteacher and/or deputy headteacher – both are notified
- High-risk alerts are escalated immediately to the DSL

Alert handling:

- All alerts are triaged based on risk level
- Safeguarding concerns are recorded on CPOMS
- Appropriate action is taken in line with the child protection policy

Review and effectiveness:

- Filtering and monitoring systems are reviewed at least annually
- Governors receive regular reports on their effectiveness

Reporting concerns:

- Staff and pupils can report concerns about filtering or monitoring systems to the DSL or headteacher
- Requests to unblock content for educational purposes must be authorised by the headteacher or DSL and risk assessed where appropriate

4. Educating pupils about online safety

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

In **Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

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

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure

- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

The safe use of social media and the internet will also be covered in other subjects where relevant. There is a central school display on safety updated regularly to reflect current issues or concerns. Termly assembly on safety.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. Extra provision, such as visual aids, pre-teaching and greater monitoring of pupils whilst online will be used to support pupils where necessary.

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. There is a dedicated area on the website that signposts parents/carers to relevant support and guidance. This policy will also be shared with parents/carers.

The school will let parents/carers 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

If parents/carers 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.

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

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 encourage them 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 classes during specific e-safety lessons, and the headteacher will discuss cyber-bullying with the school 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).

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 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

Children should not have personal electronic devices in school unless they are switched off and held in the school office.

The headteacher, and any member of staff authorised to do so by the headteacher as set out by the behaviour policy, 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 headteacher
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil'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

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

If inappropriate material is found on the device, it is up to headteacher in conjunction with the DSL 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 whether 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 (or equivalent) 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
- 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 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Mill Lodge 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Mill Lodge will treat any use of AI to bully pupils very seriously, in line with our behaviour and anti-bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of AI should be carried out following our data protection and acceptable use policies – Below is extract from Data Protection Policy concerning use of AI:

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Mill Lodge Primary School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Mill Lodge Primary School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.'

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 to 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Year 6 pupils (or those from other year groups who walk to/from school alone) are permitted to bring mobile phones to school, provided that they:

- Hand phones into the school office at the start of the day
- Collect them from the school office/ class teacher at the end of the day
- Understand that the school does not take any responsibility for lost or damaged phones
- Do not use their phone on the school site at any time

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 or the individual being banned from bringing their phone onto the school site.

The school also does not allow any other personal devices with internet access to be used on the school site. This includes, but is not limited to, the use of:

- Smartwatches
- Personal tablets
- Gaming devices

9. Staff using work devices outside school

9.1 Staff devices

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 can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- 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
- Keeping operating systems up to date by promptly installing the latest updates

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

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Work devices must be used solely for work activities.

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

9.2 Remote learning and online behaviour outside school

The school recognises that pupils access online content both in and outside of school and that online safety risks extend beyond the school day.

Pupils:

- Are expected to follow the school's acceptable use rules when accessing school systems from home
- Should behave respectfully and safely when using online platforms for learning
- Must report any concerns to a trusted adult

Staff:

- Must not communicate with pupils using personal email accounts, messaging services or social media
- Should ensure that any online teaching or communication is professional, appropriate and auditable

Parents/carers:

- Are encouraged to support their child's safe use of technology at home
- Should monitor their child's online activity where appropriate
- The school will provide guidance to parents/carers on safe use of technology at home through newsletters, the school website and workshops where appropriate.

9.3 Use of digital platforms and third-party applications

- The school ensures that all digital platforms, apps and online services used with pupils are safe and appropriate.
- All platforms must be approved by the school prior to use
- A risk assessment will be carried out where necessary, considering:
    - Safeguarding risks
    - Data protection and privacy
    - Age appropriateness
- Staff must not introduce new apps or platforms without prior approval

The school will ensure that:

- Platforms comply with data protection requirements
- Appropriate security and privacy settings are applied
- Pupils are taught how to use platforms safely

10. How the school will respond to issues of misuse

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. 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 code of employee conduct and staff disciplinary procedure. 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.

Where online safety concerns indicate a risk of harm to a pupil, this will be treated as a safeguarding concern and managed in line with the child protection and safeguarding policy.

This includes, but is not limited to:

- Online grooming or exploitation
- Exposure to extremist content or radicalisation
- Sharing of nude or semi-nude images
- Online abuse or harassment

The DSL will take lead responsibility for decision-making and may involve external agencies, including the police, where appropriate.

10.1 Data protection and privacy

The school recognises the importance of protecting personal data and ensuring privacy when using technology.

- All staff must handle personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- Personal data must only be accessed, shared or stored where necessary and authorised
- Staff must ensure that any online systems used to store or process data are secure and approved by the school

Data breaches:

- Any suspected or actual data breach must be reported immediately to the headteacher and/or data protection officer
- Breaches will be managed in line with the school's data protection policy

Images and media:

- Staff must follow school procedures when capturing, storing or sharing images of pupils
- Personal devices must not be used to take images of pupils

11. Training

11.1 Staff, governors and volunteers

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.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

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, threatening, 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 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 training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

Personal Information & Privacy

- Understand what personal information is (name, address, school, passwords, photos).
- Know never to share personal information online without a trusted adult's permission.
- Recognise that people online may not be who they say they are.
- Understand the importance of keeping passwords private and secure.

Safe Communication

- Know how to communicate kindly and respectfully online.
- Recognise unsafe or inappropriate messages.
- Understand they should not respond to messages that make them feel uncomfortable.
- Know how and when to block or report someone.

Trusted Adults & Reporting

- Identify trusted adults (parents, teachers, carers) they can talk to.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Understand the importance of telling an adult if something worries or upsets them online.
- Know that reporting is the right thing to do and they won't get in trouble for speaking up.

Online Content Awareness

- Understand that not everything online is true or reliable.
- Learn to question and check information with an adult.
- Recognise inappropriate content and know to leave it and report it.

Cyberbullying

- Understand what cyberbullying is and how it can affect others.
- Know how to respond: do not retaliate, save evidence, tell a trusted adult.
- Promote positive online behaviour and empathy.

Digital Footprint

- Understand that what they post online can stay there for a long time.
- Learn to think before posting (images, comments, videos).
- Recognise that online actions can affect themselves and others.

Safe Use of Devices & Apps

- Know basic rules for using school and home devices safely.
- Understand age restrictions on apps and games.
- Recognise in-app purchases and the need for adult permission.

Passwords & Security

- Learn how to create strong passwords (simple guidance: hard to guess, not shared).
- Understand why passwords should be kept secret (except with trusted adults).
- Recognise basic signs of scams (e.g., requests for passwords or money).

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Social media policy
- Staff code of conduct

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Pupil acceptable use policy agreement (FS2 / KS1)

When I use the computers or other technology in school I agree to stay safe by:

- I will ask a teacher or suitable adult if I want to use the computers/ tablets
- I will only use websites or applications that a teacher or suitable adult has told or allowed me to use
- I will look after the computers and any other equipment, and tell an adult immediately if I see any damage
- I will ask a teacher for help if I am unsure what to do or think I have done something wrong
- I will tell a teacher or suitable adult if I see anything that makes me feel worried, upset or confused, or that I think might upset someone else
- I will use the school computers and equipment for schoolwork only
- I understand that if I break the rules I might not be allowed to use the computers or other equipment again

Child's name: .....

Date: .....

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Appendix 2: KS2 (pupils)

Pupils acceptable use policy

(KS2)

When using the computers or other technology, we will stay safe by:

- I will ask a teacher or suitable adult if I want to use the computers/ tablets
- I will take care of the computers and tablets and tell an adult if something is broken or not working, however this may have happened
- I will only use websites and applications that a teacher or suitable adult has told me I can
- I will only use the computers and tablets for schoolwork
- I will ask for help from a teacher or a suitable adult if I am not sure what to do or if I think I may have done something wrong
- If I see anything that makes me feel worried, upset or confused, I will tell a teacher or suitable adult straightway.
- I will not share personal information online and keep my passwords private
- I understand that not everything I see online is true, and will check with a teacher or suitable adult if I am unsure about something
- I will be polite, responsible and respectful when I communicate with others and I understand that others may have different opinions to me.
- I understand that if I break the rules then I may not be allowed to use the computers or tablets again

Child's name: .....

Date: .....

Signed: .....

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

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 that 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 that 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:**

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

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?	
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms