



Online Safety Policy

Author's Name	Leona Kelly
Date Written	Autumn 2026
Next Review	Autumn 2027
Date Ratified by Governing Body	September 2026

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	4
4. Educating pupils about online safety	6
5. Educating parents/carers about online safety	7
6. Cyber-bullying	8
7. Acceptable use of the internet in school	9
8. Pupils using mobile devices in school	10
9. Staff using work devices outside school	10
10. How the school will respond to issues of misuse	11
11. Training for staff, governors and volunteers	11
12. Monitoring arrangements	11
13. Links with other policies	12
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers).....	Error! Bookmark not defined.
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)	13
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors).....	Error! Bookmark not defined.
Appendix 4: online safety training needs – self-audit for staff	16
Appendix 5: online safety incident report log	18

1. Aims

Our Trust and individual schools aim 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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this, 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** – 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), including those generated using AI, 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 statutory safeguarding guidance, [Keeping Children Safe in Education](#) from the Department for Education (DfE) and its advice for schools on:

- [Teaching online safety](#)
- [Meeting digital and technology standards](#)
- [Relationships and sex education \(RSE\) and health education](#)
- [Preventing and tackling bullying](#)
- [Searching, screening and confiscation](#)
- [Mobile phones in schools](#)

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](#), the [Children's Wellbeing and Schools Act 2026](#) 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 complies with our funding agreement and articles of association.

3. Roles and responsibilities

The Board of Trustees will ensure that appropriate arrangements are in place for online safety to be regularly discussed and monitored, including consideration of training requirements and information provided by the Designated Safeguarding Leads (DSLs).

The Board of Trustees will ensure that our schools teaches pupils how to keep themselves and others safe, including online.

The Board of Trustees will ensure that our schools have appropriate filtering and monitoring systems in place on school devices and networks and that the effectiveness of these arrangements is formally reviewed at least annually.

The Board of Trustees will have regard to the DfE's filtering and monitoring standards and ensure that appropriate school leaders, IT staff and service providers work together to support the school in meeting these standards. This includes:

- Identifying and assigning clear roles and responsibilities for managing filtering and monitoring systems.
- Reviewing filtering and monitoring provision at least annually.
- Blocking harmful and inappropriate content without unreasonably affecting teaching and learning.
- Having effective monitoring strategies that meet the school's safeguarding needs.
- Ensuring that safeguarding risks associated with new and emerging technologies, including generative AI, are considered within filtering and monitoring arrangements.

All Trustees will:

- Read and understand this policy.
- Agree and adhere to the Trust's acceptable use requirements for ICT systems and the internet.
- Ensure that online safety remains a running and interrelated theme within the school's overall approach to safeguarding and related policies and procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted to meet the needs of vulnerable children, victims of abuse and pupils with special educational needs and/or disabilities (SEND), recognising that a personalised or contextualised approach may be more appropriate than a 'one size fits all' approach.

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.

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances – for example, a confidential shared mailbox to make sure safeguarding concerns are received, monitored and acted on without delay.

3.3 The designated safeguarding lead (DSL)

Details of each 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:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and 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 ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) 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 (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 headteacher and/or 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 ICT Manager

Working alongside central team and school leaders, are external partner, One IT take on the role of ICT manager and are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and 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 each 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
- Providing Headteachers with the relevant information to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Providing Headteachers with relevant information to ensure 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 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
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) 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'

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).

4. Educating pupils about online safety

4.1 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](#) and the government's [guidance on relationships education, relationships and sex education \(RSE\) and health education \(for introduction 1 September 2026\)](#).

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 (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 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, 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.

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

4.2 Pupils will be taught practical cyber security skills

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

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

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.

Online safety will also be covered during parents' evenings.

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
- The school's expectations in respect of appropriate use of AI by pupils

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

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.

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/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the 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

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device in line with the school's searching and confiscation policy.

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

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

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

If inappropriate material is found on the device, it is up to headteacher 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/carers 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), including any image generated or altered by AI, they will not:

- View, copy, print, share, store, save, forward on, or ask a child to share or download, the image
- Delete the image or ask the pupil to delete the image
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any pupil involved

The staff member will 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](#).

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL and seek support.

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/searches and confiscation 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.

The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes' or 'deep nudes', 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.

The school will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour 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 artificial intelligence should be carried out in accordance with our AI usage policy.

7. Acceptable use of the internet in school

All pupils, staff, volunteers and Trustees are expected to follow the school's expectations regarding the acceptable use of ICT systems, devices and the internet, as set out in the relevant acceptable use agreements in the appendices.

Parents and carers will be made aware of the school's expectations for the safe and appropriate use of technology and are encouraged to support their children in following these expectations.

Visitors will be expected to follow the school's acceptable use requirements when accessing school ICT systems or the internet, where relevant.

Use of the school's internet and ICT systems must be appropriate and, for staff, volunteers and Trustees, relate to educational purposes or the legitimate duties of their role.

The school uses appropriate filtering and monitoring systems to help safeguard users and identify inappropriate or concerning online activity. Any concerns identified through monitoring will be managed in accordance with the school's safeguarding and behaviour procedures.

Further information is set out in the relevant acceptable use agreements in the appendices.

8. Pupils using mobile devices in school

Adapt this section to reflect your school's approach.

In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by the headteacher.

Where there is an arrangement by exception, any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2). Any breach of the acceptable use agreement by a pupil may trigger a sanction 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:

- 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.

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.

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 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training for 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.

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, including images generated or altered by AI, especially around chat groups
- Sharing of abusive images and pornography, including images generated or altered by AI, 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the headteacher. 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
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Mobile phones policy
- AI policy

Appendix 1: EYFS and KS1 Acceptable Use Expectations

Using technology safely in school

When I use computers, tablets, the internet or other technology in school, I will:

- Ask a teacher or adult before using technology or going online.
- Only use websites, apps and AI tools that a teacher or adult has allowed me to use.
- Follow the instructions an adult gives me when using technology.
- Tell an adult straight away if I see or hear something online that worries, upsets or confuses me.
- Tell an adult if I receive a message from someone I do not know.
- Tell an adult if I accidentally open a website, app or content that I should not be using.
- Use school computers and devices for my learning.
- Be kind and respectful to other people when using technology.
- Look after school computers, tablets and other devices and tell an adult if something is broken or not working properly.
- Only use the username and password I have been given.
- Keep my password private and not share it with my friends.
- Keep personal information about myself and other people private.
- Save my work where my teacher tells me to.
- Ask an adult before printing anything.
- Log off or close down a computer or device when I have finished using it.

Keeping everyone safe

I understand that the school uses filtering and monitoring systems to help keep everyone safe when using school devices and the internet.

If I make a mistake or see something that worries me, I know that I can tell an adult and they will help me.

If I do not follow these expectations, an adult will help me understand what has happened and what I need to do differently.

Parents and carers

Parents and carers are encouraged to talk to their children about these expectations and support the school's approach to safe, responsible and age-appropriate use of technology.

The school will provide parents and carers with information and guidance about online safety to help them support their children when using technology at home.

Appendix 2: KS2 Acceptable Use Expectations

Using technology safely and responsibly in school

When I use the school's computers, tablets, ICT systems, internet or other technology, I will:

- Use school technology and the internet responsibly and for educational purposes.
- Only use technology when a member of staff has given me permission to do so.
- Keep my usernames and passwords private and never use another person's login details.
- Keep personal information about myself and others safe and private.
- Tell a member of staff straight away if I see or receive anything online that worries, upsets or makes me feel uncomfortable.
- Tell a member of staff if I receive a message or communication from someone I do not know.
- Be kind, respectful and responsible when communicating with others online.
- Only use websites, apps, online services and AI tools that have been approved by the school.
- Use AI tools only when my teacher has given me permission and follow the instructions I have been given.
- Check information I find online and understand that not everything I see or read online, including information produced by AI, is necessarily accurate or true.
- Respect other people's work and understand that I should not copy work or present someone else's work, including AI-generated work, as my own.
- Look after school equipment and report any damage or problems to a member of staff.
- Log off or shut down a computer or device appropriately when I have finished using it.

I will not:

- Deliberately access websites, apps, games, social media, chat rooms or other online content that has not been permitted by a member of staff.
- Try to bypass the school's filtering or security systems.
- Open suspicious attachments or links or download files without permission.
- Use inappropriate, unkind, threatening or offensive language when communicating online.
- Create, access, share or send inappropriate or harmful content, including content created or altered using AI.
- Take, share or alter photographs, videos or recordings of another person without permission.
- Share personal information, photographs or videos online without permission.
- Log in to the school's systems using another person's username or password.
- Share my password with other pupils.
- Arrange to meet someone I have only communicated with online.
- Use technology to bully, upset, embarrass or harm another person.

Personal mobile phones and electronic devices

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

- I will follow the school's rules about where the device should be kept.
- I will ensure that the device is switched off and stored securely as required by the school.
- I will not access or use the device during the school day unless a member of staff has specifically given me permission to do so.
- I understand that a device may be confiscated if it is used in breach of the school's rules, in accordance with the school's Behaviour Policy.

Keeping everyone safe

I understand that the school uses filtering and monitoring systems on its networks and devices to help keep pupils and staff safe.

I understand that my use of school ICT systems and the internet may be monitored.

If I accidentally access something inappropriate or make a mistake online, I will tell a trusted adult straight away. I know that reporting something that worries me will help adults keep me and other people safe.

If I do not follow these expectations, the school will respond appropriately in line with its Behaviour, Online Safety and Safeguarding policies.

Parents and carers

Parents and carers will be made aware of the school's expectations for pupils' safe and responsible use of technology, the internet and personal electronic devices.

Parents and carers are encouraged to discuss these expectations with their child and support the school's approach to online safety and appropriate use of technology.

Appendix 3: Acceptable Use Expectations for Staff, Trustees, Volunteers and Visitors

All staff, Trustees, volunteers and visitors are expected to use the school's ICT systems, devices and internet safely, responsibly and professionally and in accordance with the school's safeguarding, data protection and online safety procedures.

When using school ICT systems, devices and the internet, I will:

- Use school ICT systems and devices appropriately and, where applicable, for educational purposes or to fulfil the duties of my role.
- Keep usernames, passwords and other login information secure and never share them with others.
- Lock or log off devices when they are left unattended.
- Take reasonable steps to ensure that school devices are secure and password-protected when used outside school.
- Store and process school information securely and in accordance with the school's Data Protection Policy.
- Only access, modify, download or share information that I am authorised to access.
- Follow the school's procedures for the safe use, storage and sharing of photographs, videos and recordings of pupils.
- Use school-approved systems for communicating about pupils and school business.
- Report any suspected cyber-security incident, data breach or loss of a school device promptly in accordance with school procedures.
- Report any online safeguarding concern involving a pupil immediately to the Designated Safeguarding Lead (DSL) or a deputy.
- Report inappropriate or harmful material encountered through school systems in accordance with school procedures.
- Ensure, where this forms part of my role, that pupils use technology safely and appropriately.
- Follow the school's requirements regarding the use of generative AI and other emerging technologies.
- Understand that use of the school's ICT systems, devices and networks is subject to appropriate filtering and monitoring to support safeguarding and cyber security.

I will not:

- Access, create, download, share or attempt to access inappropriate, illegal or harmful material.
- Attempt to bypass, disable or interfere with the school's filtering, monitoring, security or cyber-security systems.
- Use school systems or devices in a way that could compromise safeguarding, confidentiality, data protection or the security of the school's systems.
- Install unauthorised software or connect unauthorised hardware or devices to the school's network.
- Share passwords or login credentials or use another person's account.
- Access, modify or share information that I am not authorised to access.
- Share confidential information about pupils, staff, families or the school without appropriate authority.
- Use personal accounts, email addresses or messaging services to communicate with pupils.
- Take, store or share photographs, videos or recordings of pupils using personal devices unless specifically authorised in accordance with school procedures.
- Input, upload or process pupils' personal data, safeguarding information, confidential information or sensitive school data using public or unapproved generative AI tools.
- Use AI-generated information without appropriate professional judgement and checking its accuracy and suitability.
- Use AI to make decisions about pupils or produce content that compromises confidentiality, safeguarding, data protection or professional responsibilities.
- Use inappropriate, offensive, discriminatory or unprofessional language when communicating online.
- Use school systems to promote private businesses or for personal financial gain unless specifically authorised for a legitimate school purpose.

Safeguarding and professional responsibility

Any online activity or content that raises a safeguarding concern must be reported promptly to the DSL or a deputy and managed in accordance with the school's Child Protection Policy.

Staff must maintain appropriate professional boundaries when using technology and online communication, including when using social media and messaging services.

All users are expected to comply with these expectations whenever they access school ICT systems, networks or devices.

Failure by staff to comply with these expectations may be addressed through the school's appropriate disciplinary procedures. Concerns relating to Trustees, volunteers or visitors will be managed in accordance with the relevant school or Trust procedures.

Appendix 4: 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