



Two are better off than one, because together they can work more effectively.

Ecclesiastes 4:9

Online Safety Policy

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	10
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	10
11. Training	11
12. Monitoring arrangements	11
13. Links with other policies	12
14. Evaluation, Review and Revision	11
Appendix 1: Acceptable use agreement (pupils and parents/carers)	12
Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)	14
Appendix 3: Online Safety Incident Report Log	15

'Together we are great'

At Great Chesterford C. of E. Primary Academy, we aim to provide the best possible education for each child within the context of a caring Christian community. Our school values underpin all aspects of school life, including behaviour and relationships within our school. Our school values are: God's Guidance, Respect One Another, Excellent Behaviour, Aiming High and Tremendous Teamwork. Our golden rule is to 'Treat others as you would like to be treated.'

Computing and PSHE, of which e-safety and safe use of the Internet are an integral element, are taught as part of a broad and balanced curriculum, which will enable each child to develop confidently and learn and achieve to the best of his/her ability in a safe environment. The Internet is part of everyday life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience. Pupils will be taught how to use the Internet safely and show a mature and responsible approach to its use. Pupils will use age-appropriate tools to research internet content and be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1. Aims

Our school aims to:

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

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, 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 Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- › [Teaching online safety](#)
- › [Meeting digital and technology standards](#)
- › [Preventing and tackling bullying](#)
- › [Relationships and sex education \(RSE\) and health education](#)
- › [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.

This policy complies with our funding agreement and articles of association.

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 ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement.

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 must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year.. The board will review the DfE 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 their safeguarding needs.

The governor who oversees online safety is Andrew Pickering.

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 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be

appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances.

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:

- › Ensuring 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 ensure the procedures and implementation are updated and reviewed regularly
- › Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- › Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- › Working with the ICT service provider to make sure the appropriate systems and processes are in place
- › Working with the ICT service provider 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
- › Ensuring that any online safety incidents are logged (see appendix 3) 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 and anti-bullying 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 body
- › 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 Service Provider

The ICT Service Provider is responsible for:

- › Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- › Ensuring that the school's 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 3) 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 and anti-bullying 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- 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 reporting to the DSL and the ICT service provider
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) 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 relationships and behaviour policy and anti-bullying 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
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

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

Pupils will be taught about online safety as part of the curriculum. This forms part of our PSHE and Computing curriculums.

All schools have to teach:

- › Relationships education and health education in primary 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. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this or access external advisors (e.g. Crucial Crew, the 2 Johns). Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. The teaching of the computing curriculum will be monitored by the Computing Co-ordinator in liaison with teaching staff.

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 on an individual basis as required.

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

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 anti-bullying 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 to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff will 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 relationship and 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 that they have reasonable grounds for suspecting. Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

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

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

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

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), 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 relationship and 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 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 Gemini.

Great Chesterford C. of E. Primary Academy 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 in line with our anti-bullying and relationships and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment 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.

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 and 2). 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. RMSafetynet/SENSO 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 and 2.

8. Pupils using mobile devices in school

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. See our mobile phone policy for further details.

If a child requires a kindle to use in school due to a specific need, the parents/carers will provide the kindle and a signed agreement will be put in place to ensure that it is not internet enabled in school.

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 with a strong password which is not shared with anyone
- Locking the laptop (using Windows key + L) if the laptop is left unattended for any length of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always 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 2.

HfL provide IT support for the school. They are responsible for ensuring anti-virus software is up to date and operating systems are also updated. If staff have any concerns over the security of their device, they must seek advice from the HfL support desk. Work devices must be made available for updates or checks if required.

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 relationships and 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

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

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

All pupils will receive age-appropriate training on safe internet use and safeguarding issues such as cyberbullying.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection policy
- Relationships and behaviour policy
- Staff code of conduct policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Computing policy
- Anti-bullying policy
- PSHEE including RSE policy
- Mobile phone policy

14. Evaluation, Review and Revision

This policy was reviewed in September 2026 and will be reviewed annually by the Headteacher in consultation with the staff and governing body.

Signed: <i>Amy Sargeant</i> Headteacher	17 th September 2026
Signed: <i>Wazir Mughal</i> On behalf of the Governing Body	22 nd September 2026
Next review date:	September 2027

Appendix 1: Acceptable use agreement (pupils and parents/carers)

GREAT CHESTERFORD C. OF E. PRIMARY ACADEMY

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 laptops and iPads) and get onto the internet in school I will:

- Use the school computers / laptops, iPads, internet and all other technological equipment sensibly and for educational purposes.
- Ask a member of staff if I can do so before using the internet or school devices.
- Not enter chat rooms or leave messages on bulletin boards whilst using school devices.
- Only use websites that a teacher or adult has told me or allowed me to use.
- Tell my teacher immediately if I receive messages from people I don't know or I find anything that may upset or harm me or my friends.
- Use school computers for school work only.
- Look after school IT equipment and tell an adult straight away if something is broken or not working properly.
- Never share my personal details, home address or telephone numbers with anyone without the permission of my teacher, parent or carer.
- Only use the username and password I have been given and keep my passwords safe.
- Check with my teacher before I print anything.
- Be polite and use appropriate language when communicating online and using a school device.
- 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/carers 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 will support the school in making sure my child understands these. I understand that my child will be held accountable for their own actions online.

Signed (parent/carers):

Date:

Appendix 2: 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, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libelous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).
- Only use appropriate and authorized school systems to communicate electronically with pupils.
- Only conduct school business through official work emails, which are secured with strong passwords.
- Not use them in any way which could harm the school's reputation
- Not access personal social networking sites or chat rooms using school devices.
- Ensure anything I post on the School Twitter(X) feed does not identify children and follows the code of conduct policy.
- Not use any improper language when communicating online, including in emails or other messaging services.
- Not install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
- Not share my password with others or login to the school's network using someone else's details
- Not take photographs of pupils without checking permissions first.
- Not take photographs of pupils on personal devices (such as mobile phones)
- Not share confidential information about the school, its pupils or staff, or other members of the community.
- Not access, modify or share data I'm not authorised to access, modify or share.
- Not 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 lead 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.

I will use generative AI responsibly and in accordance with GDPR guidelines.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 3: 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