

E-Safety Policy



'We can and we will'

GLEBE PRIMARY SCHOOL

E-SAFETY POLICY

Table of Contents

1. Mission Statement
 2. Introduction
 3. Aims
 4. Legislation and Guidance
 5. Roles and Responsibilities
 6. Managing the School E-safety Messages
 7. E-safety in the Curriculum
 8. Cyber-bullying
 9. Examining electronic devices
 10. Security, Data and Confidentiality
 11. Managing the Internet
 12. Mobile Technologies
 13. Managing email
 14. Social Networking
 15. Safe Use of Images
 16. Misuse, Infringements and Complaints
 17. Inappropriate material
 18. Equal Opportunities
 19. Appendices
- **Appendix 1:** EYFS and KS1 acceptable use agreement (pupils and parents/carers)
 - **Appendix 2:** KS2 acceptable use agreement (pupils and parents/carers)
 - **Appendix 3:** Acceptable use agreement (staff, governors, volunteers and visitors)
 - **Appendix 4:** Online safety training needs – self audit for staff

E-Safety Policy

Mission Statement

At Glebe School, we believe in an ethos that values the whole child.

We strive to enable all children to achieve their full potential academically, socially and emotionally.

Introduction

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Whilst exciting and beneficial, all users need to be aware of the range of risks associated with the use of these technologies.

Computing and ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognize the constant and fast paced evolution of computing within our society. Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Coding
- Gaming
- Mobile devices such as iPads
- Video & Multimedia
- Artificial Intelligence (AI) applications

At Glebe we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to be safe online.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas 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
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making or sharing of nudes or semi-nudes (including images digitally altered or wholly generated by artificial intelligence such as deepfakes), harmful sexual behaviour (HSB), sexual harassment, and online bullying. This includes misogyny and other forms of inappropriate behaviour that require early intervention.
- **commerce:** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

E-Safety Policy

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;
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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](#) 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
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- The Crime and Policing Act 2026

Roles and Responsibilities

The governing body

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

E-Safety Policy

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

The governor who oversees online safety is John Buckingham

All governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).
- Ensure that online safety is a running and interrelated theme while devising and implementing our whole-school approach to safeguarding and related policies and/or procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

The Headteacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. Ensuring all staff are aware of the risks including with data, hardware and software such as cyber-attacks.

The Designated Safeguarding Lead and E-safety Lead

Details of the school's DSL are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in collaboration with the e-safety lead, 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 make sure the procedures and implementation are updated and reviewed regularly;
- Understanding the filtering and monitoring systems and processes in place on school devices and networks;
- Working with the ICT manager (IT Inspire) and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs);
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the governing board.
- Ensure school has met standards on filtering and cyber attacks.
- Ensuring staff and children are aware of cyber-attacks and are trained on the basics.
- Liaising with Inspire to ensure that standards are met in regards to cyber-attacks.
- Report any cyber-attack.

E-Safety Policy

Filtering and Monitoring Review

At least once every academic year, the member responsible for filtering and monitoring (Headteacher), supported by IT Inspire, will conduct a comprehensive review of:

- The effectiveness of the school's filtering and monitoring systems
- Whether the systems appropriately limit children's exposure to online risks
- How filtering and monitoring requirements apply to generative AI
- The school's compliance with DfE filtering and monitoring standards
- Any incidents or concerns that have arisen during the year
- Whether any adjustments are needed to filtering or monitoring arrangements

ICT management (Provided by Inspire)

is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the school's ICT systems including the server on a weekly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;
- Ensuring appropriate back up servers in event of a cyber-attack. Having in place an appropriate plan in event of cyber-attack.
- Ensuring software is up to date and licenced.
- Ensure all staff and pupil accounts are secure.
- Report any cyber-attack.

This list is not exhaustive.

Internet is provided to the school by LGFL via Virgin Media. The school has full fibre broadband which runs at 300Mbps download/upload.

The firewall is a Cisco ASA 5508 which is provided by and owned by LGfL. This is fully managed and monitored by LGfL. Filtering is also provided by LGFL. Wireless internet works throughout the school and the playground area. A technology and digital standards audit will be completed once a year to ensure the school is meeting government standards. LGFL's filtering and monitoring support ensures the school is equipped in the event of a cyber attack.

E-Safety Policy

All staff and volunteers

All staff, including contractors, agency staff and volunteers are responsible for:

- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2);
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

Parents

The school will raise parents' awareness of internet safety in letters or other communications home.

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

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

Parents 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 (appendices 1 and 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - [UK Safer Internet Centre](https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues) <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

Visitors and Members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

E-Safety Policy

Managing the School E-safety Messages

We endeavour to embed e-safety across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught. E-safety guidelines and the SMART rules will be displayed around the school and in the computing suite.

E-safety in the Curriculum

The school provides opportunities within a range of curriculum areas to teach about e-safety. Educating pupils on the dangers of technologies that may be encountered is completed as part of the e-safety curriculum and informally when opportunities arise, for example as part of a PSHE lesson or class circle time. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content, including the validity and 'realness' of content, including AI generated content

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- That social media sites have minimum ages for joining to safeguard them
- Knowing the dangers of sharing information online, how to exercise caution and the importance of privacy and location settings
- Longevity of sharing things online and that material can be circulated, with no definitive way of deleting it everywhere

E-Safety Policy

- The risks associated with making or sharing of nudes or semi-nudes, including images digitally altered or wholly generated by artificial intelligence (deepfakes)
- How generative AI applications can simulate harmful online interaction for young people

Cyber-bullying

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.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

At Glebe we 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 receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

Parents are sent up to date information on cyber-bullying so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, we 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.

Examining electronic devices

- › School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. If a staff member believes a device may contain a nude or semi-nude image (including AI-generated or altered images) or an image that it's a criminal offence to possess, they will not view the image but will confiscate the device immediately and report this to the DSL (or equivalent). The DSL will then decide what to do next, 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](#)

E-Safety Policy

Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules or commits 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 whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

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](#)

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

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and the expectations of using the internet and ICT systems.

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.

Managing the Internet

All internet activity within school is monitored and filtered through LGFL.

Whenever any inappropriate use is detected, the Safeguarding lead will be notified and the incident will be followed up in line with the school Acceptable Use Policy.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school's digital devices. If Internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research.

E-Safety Policy

Mobile Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present. Any personal mobile devices do not have access to the internet via the schools WiFi network. The school is not responsible for the loss, damage or theft of any personal mobile device.

Glebe Primary School operates a mobile phone-free environment during the school day. This means pupils do not have access to their mobile phones during lessons, breaktimes, lunchtimes, or any other school activities.

Year 6 children may bring mobile devices into school but they must be handed into class teachers at the start of the day and collected at the end of the day. Year 5 children may also bring mobile phones, if their parents have given written permission for them to walk home and to use the mobile phone, if they live a considerable distance from the school premises. These must also be handed in to the class teacher at the start of the day.

This approach ensures that:

- Pupils are not distracted by mobile phones during learning time
- Pupils can focus on face-to-face interactions during social times
- The school maintains a safe environment free from the risks associated with unsupervised mobile phone use
- The school complies with DfE guidance on mobile phones in schools and KCSIE 2026 expectations

Parents who need to contact their child during the school day should do so via the school office.

Managing email

The use of email within school is an essential means of communication for staff. Pupils currently do not access individual email accounts within school. Staff must use the school's approved email system for any school business. Staff must inform a member of SLT if they receive an offensive or inappropriate e-mail.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

E-Safety Policy

Staff should be aware of

- their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media;
- ensuring that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer.

Staff are not to post or upload any images to social media whilst on school premises. Staff should not engage or share any posts that could put the school in to disrepute. Use of social networking applications in work time, for personal use, is not permitted, unless permission has been given by the Head teacher. For no reason should a school device be used to access personal social media sites or accounts.

The school expects all staff (including governors and volunteers) to consider the safety of pupils and the risks (reputational and financial) to the school when using social media channels, including when doing so in a personal capacity. Staff are also responsible for checking and maintaining appropriate privacy and security settings of their personal social media accounts.

Staff members will report any safeguarding issues they become aware of.

When using social media, staff **must not**:

- Use personal accounts to conduct school business
- Accept 'friend requests' from, or communicate with, pupils past or present
- Complain about the school, individual pupils, colleagues or parents/carers
- Reference or share information about individual pupils, colleagues or parents/carers
- Post images of pupils
- Express personal views or opinions that could be interpreted as those of the school
- Link their social media profile to their work email account
- Use personal social media during timetabled teaching time

Any concerns regarding a member of staff's personal use of social media will be dealt with in line with the staff disciplinary policy.

Any communication received from current pupils (unless they are family members) on any personal social media accounts will be reported to the designated safeguarding lead (DSL) or member of the senior leadership team immediately.

Safe Use of Images

Creation of Videos and Photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

E-Safety Policy

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own devices must be used in this case.

Publishing pupils' images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/carers may withdraw or amend permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa on any school-based publicity materials.

Storage of Images

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops/ipads.

Misuse, Infringements and Complaints

Complaints or concerns relating to e-safety should be made to the Computing Co-coordinator and DSL.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Safeguarding lead.

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by Inspire and then forwarded to the e-safety coordinator. Depending on the seriousness of the offence; investigation may be carried out by the Headteacher or LA. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Equal Opportunities

Pupils with Additional Needs

The school endeavors to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

E-Safety Policy

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.

Internet activities are planned and well-managed for these children and young people.

Staff use of devices outside of 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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period 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 which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

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

Types of Incidents

Online Safety Incidents:

- Pupils accessing inappropriate content
- Cyberbullying
- Sharing of inappropriate images
- Concerns about radicalisation or extremism online

Cyber Security Incidents:

- Suspected phishing emails or messages
- Malware or virus infection
- Ransomware attack
- Unauthorised access attempts to systems
- Loss or theft of school devices
- Suspicious system behaviour

Data Breach Incidents:

- Personal data sent to wrong recipient
- Unauthorised access to confidential information
- Lost or stolen device containing personal data
- Data shared inappropriately (verbally, in writing, or electronically)
- Unauthorised disclosure of sensitive information

E-Safety Policy

Reporting Procedures

If you suspect an online safety incident:

1. **Do not** investigate further or attempt to view inappropriate material
2. **Immediately** report to the DSL]
3. Complete an incident log within 24 hours

If you suspect a cyber security incident:

1. **Do not** attempt to fix the issue yourself
2. **If malware is suspected:** Disconnect the device from the network (unplug ethernet/turn off WiFi) but do not turn off the device
3. **Immediately** contact IT Inspire AND inform the Headteacher
4. **Do not** continue using the affected system
5. Complete an incident log within 24 hours

If you suspect a data breach:

1. **Immediately stop** any further data being shared or accessed
2. **Secure** any physical documents or devices
3. **Immediately** report to the Headteacher
4. **Do not** attempt to retrieve or delete data without authorisation
5. Complete an incident log **within 2 hours**

Timescales

- **All incidents** must be reported immediately upon discovery
- **Data breaches** must be logged within 2 hours and assessed within 24 hours
- **Serious data breaches** may need to be reported to the ICO within 72 hours
- **Cyber security incidents** require immediate containment action
- **Online safety incidents** involving illegal material must be reported to police as soon as reasonably practicable

Pupil Reporting

Pupils should report any concerns to:

- Their class teacher
- The DSL:
- Any trusted adult in school

Pupils will not be penalised for reporting incidents in good faith, even if they were involved in the incident.

Investigation and Follow-up

All incidents will be:

- Logged in the online safety incident log
- Investigated appropriately by the DSL and/or IT Inspire
- Followed up with relevant parties (pupils, staff, parents)
- Reviewed to identify lessons learned and preventative measures
- Reported externally where required (ICO, police, local authority)

Confidentiality

Incident details will be shared only with those who need to know. Personal information will be handled in accordance with data protection legislation.

E-Safety Policy

Data Breaches and Data Protection

Any incident involving the inappropriate access, sharing, loss, or theft of personal data must be reported immediately in accordance with the school's **Data Protection Policy**.

Examples of data breaches include:

- Sending an email containing pupil information to the wrong recipient
- Losing a device containing school data
- Unauthorised access to confidential files
- Sharing personal information inappropriately

All data breaches must be reported immediately to the Headteacher and handled in accordance with the procedures set out in the school's Data Protection Policy, including timescales for reporting to the Information Commissioner's Office (ICO) where required.

For full data breach procedures, including reporting timescales and ICO notification requirements, refer to the school's **Data Protection Policy**.

Reviewed: October 2026

To be reviewed: October 2027

E-Safety Policy

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

ACCEPTABLE USE OF THE SCHOOL'S ICT FACILITIES AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS - KS1

Name of pupil: _____

When I use the school's ICT systems and facilities (such as computers, tablets and other equipment) and access the internet in school, I will:

- Ask a teacher or adult for permission before using them.
- Only use websites and online resources that a teacher or adult has allowed me to use.
- Use school computers and equipment for schoolwork and learning activities only.
- Be kind and respectful to others when using technology.
- Look after school ICT equipment and tell a teacher straight away if something is broken or not working properly.
- Only use the username and password I have been given.
- Try my best to remember my username and password and keep them safe.
- Never give my personal information (such as my name, address or telephone number) to anyone without permission from my teacher or parent/carer.
- Save my work on the school network where appropriate.
- Check with my teacher before printing anything.
- Log off or shut down a computer or device when I have finished using it.
- Tell a teacher or trusted member of staff immediately if I find anything online that upsets me, may harm me or others, or if I receive messages from people I do not know.

I will not:

- Use the school's ICT systems or facilities without permission from a teacher or responsible adult.
- Use them to break school rules.
- Access inappropriate websites or online content.
- Access social networking sites unless directly permitted by a teacher for a learning activity.
- Use chat rooms.
- Open email attachments or click on email links without checking with a teacher first.
- Use unkind, rude or inappropriate language when communicating online or by email.
- Send or share photos, videos or livestreams of myself or others.
- Share my password with anyone else or log in using someone else's username or password.
- Bully, harass or upset other people online.

I understand that:

- The school will monitor the websites I visit and how I use the school's ICT systems and equipment to help keep me safe and ensure I follow the rules.
- I must tell a teacher or member of staff immediately if I find anything online that is upsetting, harmful, inappropriate or wrong.
- I must always use the school's ICT systems and internet responsibly.
- There will be consequences if I do not follow these rules.
- The school may discipline me if I do certain unacceptable things online, even when I am not in school.

Signed (pupil): _____

Date: _____

Parent/carer agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands and follows these rules.

Signed (parent/carer): _____

Date: _____

E-Safety Policy

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil: _____	
I will read and follow the rules in the Acceptable Use Policy.	When I use the school's ICT systems (including computers, tablets and other devices) and access the internet, I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only. • Only use them when a teacher is present, or with a teacher's permission. • Keep my username and password safe and not share these with others. • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer. • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others. • Use appropriate and respectful language when communicating online. • Always log off or shut down a computer or device when I am finished using it.
I will not:	• Use the school's ICT systems for non-educational purposes unless authorised by a member of staff. • Use ICT facilities to break school rules. • Access any inappropriate websites or content. • Access social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher. • Use any inappropriate language when communicating online, including in emails. • Share images, videos or livestreams of others using school ICT systems. • Log in to the school's network using someone else's details. • Share my password with others. • Bully, harass or intimidate other people online. • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.
If I bring a personal mobile phone or other personal electronic device into school:	• I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission. • I will use it responsibly, and will not access any inappropriate websites, content or materials, or use inappropriate language when communicating online.
I understand that:	• The school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I must immediately report any material or behaviour online that may upset, distress or harm me or others. • There will be consequences if I do not follow these rules. • The school may discipline me for certain unacceptable online behaviours, even when I am not in school.
I agree to use the school's ICT systems and internet responsibly at all times.	
Signed (pupil):	_____
Date:	_____
Parent/carer's agreement:	I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these expectations and follows them.
Signed (parent/carer):	_____
Date:	_____

E-Safety Policy

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

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

Name of staff member/governor/
volunteer/visitor: _____

When using the school's ICT facilities and systems and accessing the internet in school, or outside school on a work device (if applicable), I will:

- Only use the school's ICT systems and internet for educational purposes or for fulfilling the duties of my role.
- Take all reasonable steps to ensure that work devices are secure, password-protected and used in accordance with the school's data protection requirements.
- Keep all data securely stored in line with this policy and the school's data protection policy.
- Report any material that may upset, distress or harm pupils or others to the Designated Safeguarding Lead (DSL) and ICT Manager.
- Ensure that pupils in my care use the school's ICT systems and internet responsibly and safely.

I will not:

- Access, or attempt to access, any illegal, unauthorised, inappropriate or harmful material.
- Use the school's ICT systems in any way that could damage the school's reputation.
- Access social networking sites or chat rooms unless authorised for a legitimate school purpose.
- Use improper, offensive or inappropriate language when communicating online, including by email or other messaging services.
- Install 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 another person's credentials.
- Take photographs of pupils without prior authorisation from the appropriate member of staff and in accordance with school procedures.
- Share confidential information about the school, its pupils, staff or other members of the school community.
- Access, modify, copy or share data that I am not authorised to access, modify or share.
- Promote any private business or commercial activity unless it is directly related to the school's work.

I understand that:

- The school will monitor the websites I visit and my use of the school's ICT facilities, systems and internet access.
- I am responsible for ensuring that all school data remains secure when working on or off site.
- I must notify the DSL and ICT Manager if a pupil reports finding material that may upset, distress or harm themselves or others, or if I encounter such material myself.
- Failure to comply with this agreement may result in disciplinary action and/or withdrawal of access to school ICT systems.

I agree to use the school's ICT systems and internet responsibly, professionally and in accordance with all school policies at all times.

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

Date: _____

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

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
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?	

E-Safety Policy

Appendix 5: online safety incident report log

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