



Glenfield Primary School

Online Safety Policy

Date of Review	September 2026
Next Review Date	September 2027
Headteacher	Sukhi Tibbles
Chair of Governors	Tessa Wildgoose
Signed	Signed Copy held centrally
Date	1.9.2027

1. Aims

Glenfield Primary School is committed to safeguarding and promoting the welfare of all pupils and recognises that technology presents both opportunities and risks. Online safety is an integral part of safeguarding and requires a whole-school approach involving pupils, staff, governors and parents.

The aims of this policy are to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety which empowers the whole school community to benefit safely from technology.
- Establish clear mechanisms to identify, respond to, record and escalate online safety concerns.
- Ensure compliance with statutory safeguarding guidance and best practice.
- Promote safe, responsible and respectful use of digital technologies.
- Protect children from harmful online content, contact, conduct and commerce risks, including emerging risks associated with artificial intelligence (AI).

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 including:

-Pornography, extremist material, racism, misogyny, violence against women and girls (VAWG), self-harm and suicide content, anti-Semitism, radicalisation, misinformation, disinformation, conspiracy theories, AI-generated harmful content, manipulated or deepfake images and videos

Contact

Being subjected to harmful online interaction with others, including:

-Peer pressure, cyberbullying, online grooming, coercion, exploitation, adults posing as children, criminal, sexual or financial exploitation

Conduct

Personal online behaviour that increases the likelihood of harm, including:

-Online bullying, sexual harassment, abusive or misogynistic behaviour, sharing personal information, sharing or creating inappropriate images, consensual and non-consensual sharing of nude and semi-nude images, misuse of generative AI tools, creation or sharing of manipulated or deepfake content

Commerce

Risks such as:

-Online gambling, phishing, fraud, financial scams, inappropriate advertising, malicious software and malware

If staff believe any member of the school community may be at risk of online exploitation, fraud or cybercrime, concerns will be reported in line with safeguarding procedures.

2. Legislation and guidance

This policy is based on:

- Keeping Children Safe in Education 2026 (KCSIE)
- Teaching Online Safety in Schools
- Relationships Education, Relationships and Sex Education (RSE) and Health Education
- Preventing and Tackling Bullying
- Prevent Duty Guidance
- Working Together to Safeguard Children
- The Education Act 1996
- The Education and Inspections Act 2006
- The Equality Act 2010

The school recognises that safeguarding incidents can take place both online and offline and that online safety is an essential component of effective child protection arrangements.

3. Roles and responsibilities

The Governing Body

The Governing Board will:

- Ensure online safety arrangements are effective and regularly reviewed.
- Receive regular safeguarding reports relating to online safety.
- Ensure appropriate filtering and monitoring systems are in place.
- Seek assurance that filtering and monitoring systems are effective and proportionate.
- Ensure online safety education is embedded across the curriculum.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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
- Ensure safeguarding measures reflect emerging technologies and risks.
- Ensure that they have read and understood this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and internet (*Appendix 1*)

An annual review of filtering and monitoring arrangements will be completed and reported to governors. This review will evaluate effectiveness, identify emerging risks and determine whether additional controls are required.

The headteacher

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

They will:

- work with the ICT Lead and other staff as necessary to address online safety issues or incidents
- Manage all online safety issues and incidents in line with the school child protection policy
- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Update and deliver staff training on online safety
- Liaise with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the Governing Body

The ICT Lead (LEAD IT)

The ICT lead is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness, reflect the most up to date risks 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

4. Filtering and monitoring

Glenfield Primary School recognises that effective filtering and monitoring systems are essential safeguarding measures.

Current Systems

- Firewall: Nasstar
- Filtering: Netsweeper
- Antivirus: Sophos
- Monitoring: Senso

The school will:

- Review filtering and monitoring arrangements regularly.
- Carry out and document a formal review at least annually.
- Ensure systems reflect the latest safeguarding risks.
- Monitor for searches linked to self-harm, extremism, radicalisation, bullying, exploitation and other safeguarding concerns.
- Ensure that AI-enabled platforms accessed through school systems are subject to appropriate safeguards and content controls.

The Headteacher, DSL, ICT Lead and safeguarding governor will collectively oversee the effectiveness of filtering and monitoring arrangements.

Artificial Intelligence (AI)

Glenfield Primary School recognises that generative AI technologies present both opportunities and safeguarding risks.

The school will:

- Teach pupils to think critically about AI-generated content.
- Help pupils understand that AI responses may be inaccurate, biased or misleading.
- Educate pupils about deepfakes and manipulated content.
- Ensure AI tools used in school are age-appropriate and risk assessed.
- Respond appropriately to incidents involving AI-generated harmful content, cyberbullying or image-based abuse.
- Review developments in AI technology as part of ongoing safeguarding practice.

Staff should remain vigilant to the misuse of generative AI tools and report safeguarding concerns through established procedures.

Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the Early Years Foundation Stage (EYFS) Curriculum and National Curriculum.

In **EYFS**, pupils will be taught to

Use technology safely and understand the importance of asking permission to use electronic devices and online games

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

In **Key Stage 2**, pupils will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to critically consider the information being presented online and whether it is factual or not
- 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

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.

In addition to statutory curriculum requirements, pupils will be taught:

- how to identify misinformation and disinformation
- how to critically evaluate online information
- how algorithms and AI-generated content can influence opinions
- the risks posed by social media, gaming and messaging platforms
- how to report online concerns
- how to establish healthy online relationships
- how to recognise online exploitation and coercion
- the importance of respect, kindness and responsibility online

Where appropriate, learning will be adapted to meet the needs of vulnerable pupils and those with SEND.

Working with Parents

The school will support parents by providing information, guidance and updates about:

- social media platforms
- online gaming
- messaging services
- artificial intelligence
- deepfakes
- misinformation and disinformation
- online safety trends and emerging risks

This policy will be published on the school website and made available on request.

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

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)

Cyberbullying, Online Harassment and Image-Based Abuse

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 one person or group by another person or group, where the relationship involves an imbalance of power.

The school recognises that online abuse can take many forms including:

- cyberbullying
- online sexual harassment
- misogynistic behaviour
- discriminatory abuse
- image-based abuse
- sharing manipulated or AI-generated images
- coercive behaviour through digital platforms

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. Children will understand the importance of being an active bystander and reporting cyber-bullying or other online conduct issues.

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 are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

Mobile Devices in School

The school maintains clear expectations regarding the use of mobile devices.

Pupils should not bring mobile phones to school unless agreed with the Headteacher. Where mobile devices are brought to school, they must be handed to the class teacher and stored securely.

Staff must not use mobile phones while supervising pupils except in emergencies or where authorised for educational purposes.

Mobile phone arrangements will be reviewed annually as part of the school's safeguarding and online safety procedures.

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
- Making sure devices are locked when left unattended
- Only using work devices for work activities

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 1.

Staff Training

All staff will:

- Receive annual safeguarding and online safety training.
- Receive updates throughout the year regarding emerging risks.
- Read and confirm that they have understood Part One of Keeping Children Safe in Education 2026.
- Understand their responsibilities regarding online safeguarding, filtering and monitoring.
- Be aware of the risks associated with AI-generated content, deepfakes, online harassment and exploitation.

The school will maintain records of training and staff compliance.

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

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to read and agree to 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.

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

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 behaviour policy. The incident will also be logged via CPOMS. 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.

Monitoring Arrangements

This policy will be reviewed annually by the governing body.

Appendix 1 – Online safety policy

Acceptable Use Agreement – Staff

Note: All Internet and email activity is subject to monitoring

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking –Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become “friends” with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME :

SIGNATURE :

DATE :

Appendix 2

Acceptable Use Policy for Primary Pupils



ZIP IT

Keep your personal stuff private and think about what you say and do online.



BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.



FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

To keep me safe whenever I use the internet or email, I promise...



- to keep my password private and not to use anyone else's login
- to keep my name, age, address and other personal information private
- not to click on any links or files that I do not understand or trust
- to tell an adult about any strange messages or upsetting internet pages
- to tell someone I trust if someone asks to meet me offline
- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy
- I will use school computers for school work and not to upset or be rude to other people
- I will tell a teacher straight away if I see a website that is not my work or receive emails from people I don't know.
- I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly
- I will only use the username and password I have been given and I will keep them secret
- I will save only school work on the school network and will check with my teacher before printing
- I will log off or shut down a computer when I have finished using it
- I understand that my behaviour will be monitored
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own
- I will check that information I use from the internet is from a trusted website

If I break these rules...

- I understand that the school's behaviour guidelines will be followed.