United Through Jesus in Faith, Love and Learning

POLICY - E-SAFETY

Date of Adoption:	SEPTEMBER 2026	Date of Review:	recommended annually
Author:	DHT	Committee responsible for Review:	FGB
Version:	v1	Date Approved:	15.09.2026
Updates:	updated in line with KCSIE 2026		

Office use only:

E SAFETY POLICY

This online safety policy is linked to our:

- Child protection and safeguarding policy.
- Pupil admissions booklet.
- Positive behaviour and anti-bullying policy.
- Staff code of conduct and disciplinary procedures.
- Data protection policy and privacy notices.
- Complaints procedure.
- IT and internet acceptable use agreements.
- Computing curriculum.
- Relationships education and PSHE curriculum.
- Filtering and monitoring arrangements.
- Mobile phone and personal device arrangements.

Contents

- Aims
- Legislation and guidance
- Roles and responsibilities
- Filtering and Monitoring
- Generative Artificial Intelligence
- Educating children about online safety
- Educating parents about online safety
- Cyberbullying
- Acceptable use of the internet in school
- Pupils using mobile devices in school
- Staff using work devices outside school
- How the school will respond to issues of misuse
- Training
- Monitoring arrangements

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

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

Appendix 3: acceptable use agreement for staff, governors and volunteers

1. Aims

Our school aims to:

Establish a whole-school approach to online safety that protects and educates pupils, staff, volunteers, governors and families.

Maintain effective arrangements for identifying, reporting, responding to and escalating online safeguarding concerns.

Provide appropriate filtering and monitoring systems across school-managed devices and networks.

Ensure that responsibilities for online safety, filtering and monitoring are clearly assigned and understood.

Provide age-appropriate online safety education through computing, PSHE, relationships education and the wider curriculum.

Recognise and respond to emerging risks, including generative artificial intelligence, manipulated images, harmful online influences, misinformation and online exploitation.

Ensure that online safety arrangements meet the needs of pupils with SEND and other vulnerabilities.

Support parents and carers in understanding online risks and keeping children safe.

Review online safety arrangements regularly to reflect changes in technology, safeguarding risks and statutory guidance.

The 4 key categories of risk

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

Content – Exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.

Contact – Harmful online interaction with other users or generative artificial intelligence applications that simulate human interaction. This includes peer pressure, grooming, exploitation, inappropriate advertising and adults pretending to be children or young people.

Conduct – Online behaviour that increases the likelihood of harm, including cyberbullying and creating, sending, receiving or sharing explicit images, including images generated or manipulated using artificial intelligence.

Commerce – Risks associated with online gambling, inappropriate advertising, phishing, financial scams, in-game purchases and other forms of online financial exploitation.

The school recognises that these risks frequently overlap and that children may experience harm through several categories simultaneously.

2. Legislation and guidance

This policy is based on current statutory guidance and legislation, including:

- *Keeping Children Safe in Education 2026*.
- *Working Together to Safeguard Children*.
- The Department for Education's filtering and monitoring standards for schools and colleges.
- The Department for Education's cybersecurity standards for schools and colleges.
- Department for Education guidance on teaching online safety in schools.
- Department for Education guidance on relationships education, relationships and sex education and health education.
- Department for Education guidance on searching, screening and confiscation.
- Department for Education guidance on mobile phones in schools.
- Department for Education guidance on generative artificial intelligence in education and relevant AI product safety standards.
- UK Council for Internet Safety guidance on sharing nudes and semi-nudes.
- The Prevent duty and associated statutory guidance.
- The national curriculum computing programmes of study.
- The Equality Act 2010.
- The Data Protection Act 2018.
- The UK General Data Protection Regulation.
- The Data (Use and Access) Act 2025.
- The Online Safety Act 2023.
- The Education and Inspections Act 2006 and the Education Act 2011, where relevant to searching, screening and confiscation.
- The Early Years Foundation Stage statutory framework, where relevant to pupils in Reception and any school-based early years provision.

This policy should be read alongside the school's child protection and safeguarding policy, behaviour policy, staff code of conduct and data protection arrangements.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall strategic responsibility for safeguarding and online safety.

The governing board will:

- Ensure that the school has effective online safety arrangements that reflect current statutory guidance.
- Ensure that appropriate filtering and monitoring systems are in place across school-managed devices and networks.
- Ensure that filtering and monitoring arrangements are reviewed at least once during every academic year.
- Receive assurance that filtering and monitoring checks are completed, recorded and acted upon.
- Ensure that online safety is reflected in the school's child protection policy, curriculum, staff training and parental engagement.
- Ensure that all staff, including those who do not work directly with children, read Part One of the current edition of *Keeping Children Safe in Education*.
- Ensure that safeguarding and online safety teaching are adapted where necessary for pupils with SEND and other vulnerabilities.
- Receive appropriate reports about online safety incidents, trends, filtering and monitoring arrangements and actions taken.
- Ensure that governors receive suitable safeguarding and online safety training.

The Safeguarding Governor has responsibility for overseeing online safety, including the effectiveness of filtering and monitoring arrangements.

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 IT systems and the internet (appendix 3)

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

Governors will ensure that filtering and monitoring arrangements are reviewed at least annually and will receive appropriate training to understand the scope and limitations of these systems.

3.2 The headteacher

The headteacher is responsible for ensuring that this policy is implemented consistently throughout the school.

The headteacher will:

- Ensure that staff understand their responsibilities for online safety.
- Ensure that online safety is embedded within safeguarding practice, the curriculum and staff training.
- Identify the senior leader responsible for filtering and monitoring arrangements.
- Ensure that filtering and monitoring provision is reviewed at least annually.
- Ensure that appropriate action is taken when online safety concerns, safeguarding incidents or technical weaknesses are identified.
- Ensure that parents and carers receive relevant information about online safety.
- Ensure that appropriate arrangements are in place for oversight during the absence of the DSL or other responsible staff.

The senior leadership team member responsible for filtering and monitoring is Rebecca Jackson, Deputy Headteacher and Designated Safeguarding Lead.

3.3 The designated safeguarding lead

Details of the designated safeguarding lead and deputy designated safeguarding leads are set out in the school's child protection and safeguarding policy.

The DSL takes lead responsibility for safeguarding and online safety. This includes:

- Ensuring that staff understand this policy and follow the school's reporting procedures.
- Receiving, assessing and responding to online safeguarding concerns.
- Ensuring that online safety concerns and incidents are recorded promptly on CPOMS.
- Reviewing relevant filtering and monitoring alerts and ensuring appropriate safeguarding action is taken.
- Working with the designated senior leader, IT technician and governors to review filtering and monitoring arrangements.
- Ensuring that appropriate arrangements are in place for deputy DSLs to access and respond to safeguarding alerts when the DSL is unavailable.
- Identifying patterns and emerging risks arising from online safety incidents.
- Ensuring that incidents involving online bullying, exploitation, harmful sexual behaviour, manipulated images or AI-generated material are managed in accordance with safeguarding procedures.
- Liaising with children's social care, the police, the local authority and other agencies when necessary.
- Supporting the delivery of staff training and age-appropriate pupil education.
- Providing appropriate reports and assurance to the governing board.

Where the DSL is unavailable, an appropriately trained deputy DSL will assume responsibility for receiving and responding to urgent online safeguarding concerns.

3.4 IT Technician and Technical Responsibilities

The school's internal IT technician is responsible for:

- Maintaining appropriate filtering and monitoring systems across school-managed devices and networks.
- Ensuring that filtering arrangements block illegal, harmful and inappropriate content without unreasonably restricting legitimate teaching and learning.
- Undertaking and recording technical checks on relevant devices, locations and user accounts.
- Providing filtering and monitoring reports to the designated senior leader and DSL.
- Alerting the DSL promptly to technical failures, significant risks or safeguarding concerns.
- Maintaining appropriate cybersecurity protections, including software updates, access controls and malware protection.
- Ensuring that new devices, platforms and software are compatible with existing safeguarding and security arrangements before use.
- Supporting the annual filtering and monitoring review.
- Supporting risk assessments relating to new technologies, including generative artificial intelligence.
- Investigating and resolving technical weaknesses or security incidents.

Technical responsibility for maintaining systems does not replace the safeguarding responsibilities of the governing board, senior leaders or the DSL.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including supply staff, trainee teachers, agency staff, volunteers and contractors where relevant, are responsible for:

- Reading and following the school's online safety and safeguarding policies.
- All staff, including those who do not work directly with children, must read Part One of the current edition of *Keeping Children Safe in Education*. Volunteers and contractors will receive safeguarding information appropriate to their roles.
- Understanding the school's filtering and monitoring arrangements and how to report concerns.
- Reporting online safeguarding concerns immediately to the DSL or deputy DSL.
- Recording concerns on CPOMS in accordance with school procedures.
- Complying with the school's acceptable use agreements and staff code of conduct.
- Ensuring that pupils follow age-appropriate acceptable use expectations.

- Responding appropriately to concerns about online bullying, exploitation, harmful sexual behaviour, misogyny, racism and other discriminatory behaviour.
- Recognising that safeguarding concerns may involve AI-generated content, manipulated images, online impersonation or harmful interactions with chatbots.
- Maintaining an attitude of professional curiosity and recognising that online abuse can affect any child.
- Following appropriate procedures when a concern involves nude or semi-nude images.
- Reporting concerns about the conduct of colleagues, volunteers or contractors in accordance with the school's safeguarding procedures.

This list is not intended to be exhaustive.

3.6 Parents and carers

Parents and carers are expected to:

- Support the school's approach to online safety.
- Familiarise themselves with relevant acceptable use expectations.
- Discuss age-appropriate online safety expectations with their child.
- Raise concerns about online bullying, harmful content, inappropriate contact or other online risks with the school.
- Inform the school where an online issue outside school may affect a child's safety, wellbeing or relationships in school.

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

3.7 Visitors and members of the community

Visitors, contractors, trainee teachers and members of the community who use school devices, networks or online systems must comply with the school's safeguarding and acceptable use requirements.

Where appropriate, they will be informed of relevant filtering and monitoring arrangements and expected to follow the school's procedures for reporting concerns.

4. Filtering and Monitoring

The school maintains appropriate filtering and monitoring systems across school-managed devices and networks to reduce pupils' exposure to illegal, harmful and inappropriate online content.

Filtering and monitoring arrangements form part of the school's wider safeguarding responsibilities and are overseen by the governing board, designated senior leader, DSL and IT technician.

The school's filtering and monitoring arrangements will:

- Block access to illegal, harmful and inappropriate online material.
- Consider pupils' ages, vulnerabilities and safeguarding needs.
- Avoid unreasonable restrictions that prevent legitimate teaching, learning or safeguarding education.
- Apply across relevant school-managed internet-connected devices, user accounts and school locations.
- Provide relevant monitoring information and safeguarding alerts to appropriate staff.
- Be reviewed following significant safeguarding incidents or technological changes.

Annual review

Filtering and monitoring provision will be reviewed at least once during every academic year.

The review will be led by the designated senior leader, with support from the DSL and IT technician. The governor responsible for online safety will be involved in reviewing assurance and any resulting actions.

The review will consider:

- Whether current systems adequately meet the needs of pupils and staff.
- The age range of pupils and the needs of pupils with SEND or other vulnerabilities.
- Relevant safeguarding incidents, alerts and emerging risks.
- Whether filtering works across all relevant devices, locations and user groups.
- The effectiveness of monitoring arrangements and reporting procedures.
- Any use of remote access, personal devices or school devices taken off site.
- New or proposed technologies, including generative artificial intelligence.
- Whether arrangements allow appropriate curriculum teaching without excessive blocking.
- Staff training needs.
- Any required improvements to systems, procedures or policies.

Checks and record-keeping

Technical and safeguarding checks will be completed at intervals determined by the school's risk assessment.

Records of checks will include:

- The date of the check.
- The name and role of the person completing it.
- The devices, locations, user accounts or systems tested.
- Any weaknesses or safeguarding concerns identified.
- Actions taken and the date on which issues were resolved.

Additional checks will be undertaken following:

- Significant safeguarding incidents.
- Changes to network settings or system configuration.
- The introduction of new devices, software or online platforms.
- Major software or security updates.
- Changes to remote access or personal device arrangements.
- The introduction of generative AI tools.

Responding to alerts

Filtering and monitoring alerts that indicate a potential safeguarding concern will be reviewed promptly by the DSL or an appropriately trained deputy.

Where a concern relates to a pupil's safety or wellbeing, the matter will be recorded on CPOMS and managed in accordance with the school's child protection and safeguarding policy.

Urgent concerns will be escalated immediately to relevant agencies where appropriate.

If filtering or monitoring systems fail, the designated senior leader and DSL will assess whether access to affected devices or systems should be restricted until appropriate protection is restored.

5. Generative Artificial Intelligence

The school recognises that generative artificial intelligence can offer educational benefits but also presents safeguarding, privacy, security and ethical risks.

Generative AI tools may produce text, images, audio or video that appear convincing but are inaccurate, misleading, discriminatory or harmful. Some tools may simulate human interaction or create manipulated images, including fabricated nude or semi-nude images.

Any generative AI tool used by staff or pupils for school purposes must be approved by the headteacher or designated senior leader before use.

Approval will consider:

- Age suitability.
- Safeguarding risks.
- Privacy and data protection.
- The accuracy and reliability of generated material.
- Compatibility with filtering and monitoring arrangements.
- Appropriate supervision.
- Intellectual property and copyright considerations.
- Whether the tool is suitable for the intended educational purpose.

Staff must not upload or enter confidential, sensitive or identifiable information about pupils, families or colleagues into an AI system unless this has been specifically authorised and complies with the school's data protection arrangements.

Pupils may only use approved AI tools under appropriate supervision and in accordance with the school's acceptable use requirements.

Any concern involving AI-generated harmful content, impersonation, manipulated images, simulated relationships or fabricated nude or semi-nude images must be reported immediately to the DSL and recorded in accordance with safeguarding procedures.

The school will review the use of AI tools regularly and ensure that emerging risks inform staff training, curriculum planning and parental communication.

6. Educating pupils about online safety

Online safety will be taught as a progressive and interconnected theme through computing, relationships education, PSHE and the wider curriculum.

Teaching will be age-appropriate and responsive to pupils' developmental stages, individual needs and emerging online risks.

The school will use relevant national curriculum requirements, statutory relationships education expectations and current safeguarding guidance when planning online safety education.

The online safety curriculum will be reviewed regularly to ensure that pupils develop the knowledge, understanding and confidence needed to stay safe.

In Key Stage 1, pupils will be taught to:

Use technology safely, respectfully and responsibly.
Keep personal information private.
Understand that people online may not always be who they claim to be.

Recognise when online content, messages or interactions make them feel uncomfortable.
Identify trusted adults who can help them.
Understand that online images, voices and information can sometimes be changed or created using technology.
Recognise the importance of kindness and respectful communication online.
Understand that some online games and services contain advertising or requests to spend money.
Stop, close the screen or move away and tell a trusted adult if something online worries them.

Pupils in Key Stage 2 will be taught to:

Use technology safely, respectfully and responsibly.
Recognise acceptable and unacceptable online behaviour.
Identify how and where to report concerns about online content, contact or conduct.
Understand the risks of communicating with people they do not know.
Recognise grooming, manipulation, pressure and requests for personal information.
Understand how online information can be misleading, inaccurate or deliberately manipulated.
Recognise that artificial intelligence can generate realistic text, images, voices and videos.
Understand the risks associated with chatbots, impersonation and manipulated images.
Recognise online bullying, racism, misogyny and other discriminatory behaviour.
Understand the importance of consent when sharing photographs or personal information.
Recognise age-appropriate risks associated with sharing images and know how to seek help.
Understand the risks of harmful online challenges, inappropriate content and extremist material.
Identify online scams, phishing, gambling-like features and inappropriate commercial pressures.
Understand how online behaviour can affect wellbeing, relationships and personal safety.
Seek help promptly when they or someone else experiences an online concern.

By the end of primary school, pupils will know:

That people may behave differently online and may conceal or misrepresent their identity.
That respectful behaviour and appropriate boundaries apply equally online and offline.
How to recognise and report harmful content, inappropriate contact and unsafe online behaviour.
How personal information is collected, shared and used online.
How to protect privacy and make sensible decisions about sharing information.
That online information, images, videos and voices can be manipulated or generated using artificial intelligence.
How to question the reliability of online information and recognise misinformation.
That online bullying, racism, sexism and discriminatory behaviour are unacceptable.
How online friendships and interactions can create risks.
How to seek help if they experience pressure, threats, exploitation or unwanted contact.
That they will be listened to and supported if they report an online concern.

Pupils with SEND and additional vulnerabilities

Online safety teaching will be adapted where necessary for pupils with SEND, communication difficulties, social or emotional vulnerabilities and other additional needs.

Staff will recognise that some pupils may find it more difficult to identify manipulation, understand online relationships, recognise misleading information or communicate concerns.

The DSL, SENCO and class teachers will work together to provide appropriate adaptations, additional support or individual risk assessments where necessary.

Reporting routes will be explained in ways that are accessible to individual pupils.

7. Educating parents about online safety

The school will work in partnership with parents and carers to promote safe and responsible use of technology.

Information about online safety will be shared through:

- School newsletters.
- The school website.
- Parent information evenings and workshops.
- Safeguarding updates.
- Information shared when new risks or online trends emerge.
- Direct communication where an individual concern affects a pupil.

Information for parents and carers may cover:

- Online gaming and messaging platforms.
- Age restrictions and parental controls.
- Online bullying and harmful content.
- Privacy settings and sharing personal information.
- Generative artificial intelligence and manipulated images.
- Harmful online influences, including misogynistic or discriminatory content.
- Grooming, exploitation and inappropriate online contact.
- Screen time and digital wellbeing.
- Reporting online concerns.
- The school's filtering and monitoring arrangements.

Where pupils are asked to access online platforms or complete online learning activities at home, parents and carers will be informed about the platforms involved and any expected interaction with school staff.

Parents and carers should raise any online safety concern with the class teacher, DSL, deputy DSL or headteacher.

Where appropriate, the school will signpost families to current resources provided by organisations such as the UK Safer Internet Centre, Childnet and the National Crime Agency's CEOP Education programme.

8. Cyberbullying

8.1 Definition

Cyberbullying is bullying that takes place using digital technology, including social media, messaging applications, online games, email, image sharing platforms and other online services.

It may involve repeated harmful behaviour, threats, intimidation, humiliation, exclusion, impersonation, discriminatory comments or the circulation of harmful images or messages.

A single online incident can have a significant and continuing impact if content is widely shared, remains accessible or causes serious distress.

Cyberbullying may overlap with other safeguarding concerns, including racism, misogyny, harassment, exploitation and harmful sexual behaviour.

8.2 Preventing and addressing cyberbullying

The school will teach pupils how to recognise cyberbullying, respond safely and report concerns.

Pupils will be encouraged to report incidents affecting themselves or others, including incidents occurring outside school where these affect a pupil's safety, wellbeing or relationships.

Class teachers will address online respect and cyberbullying through computing, PSHE, relationships education and wider class discussion.

Staff will challenge online behaviour involving sexism, misogyny, racism, discriminatory language, sexual harassment or harmful stereotypes.

Such behaviour will not be dismissed as banter, a joke or a normal part of growing up.

Reports of cyberbullying will be assessed to determine whether they should be managed through the school's behaviour procedures, safeguarding procedures or both.

The DSL will consider:

- The safety and wellbeing of the affected child.
- Whether other pupils may be at risk.
- Whether the behaviour involves harassment, exploitation, sexual content or discrimination.
- Whether the behaviour indicates exposure to harmful online influences.
- Whether the child displaying harmful behaviour also requires support.
- Whether parents, children's social care, police or other agencies should be involved.

Incidents will be recorded on CPOMS and reviewed to identify patterns or recurring concerns.

8.3 Examining electronic devices

Searches of electronic devices will only be undertaken in accordance with current Department for Education guidance, the school's behaviour policy and safeguarding procedures.

Staff should seek advice from the DSL or a senior leader before examining electronic data where a safeguarding concern is suspected.

Where an incident involves or may involve nude or semi-nude images of a child, including images that have been digitally altered or generated using artificial intelligence, staff must:

- Report the concern immediately to the DSL or deputy DSL.
- Avoid viewing the image unless doing so is unavoidable and justified under current national guidance.
- Never copy, print, forward or share the image.
- Avoid deleting material that may constitute evidence unless advised that this is appropriate.
- Secure the device where necessary.
- Follow guidance from the DSL, police or children's social care.
- Record the safeguarding concern on CPOMS without uploading or attaching the image itself.

All incidents involving the making or sharing of nude or semi-nude images will receive a safeguarding response, whether the sharing was consensual or non-consensual.

Where appropriate, a device may be confiscated and preserved for police inspection.

The school will follow current Department for Education guidance on searching, screening and confiscation and UK Council for Internet Safety guidance on sharing nudes and semi-nudes.

9. Acceptable use of the internet in school

Pupils, parents, staff, volunteers, governors and relevant visitors are expected to comply with the school's acceptable use requirements.

School devices, networks and online systems must be used for appropriate educational or professional purposes.

Users must not:

- Access or attempt to access illegal, harmful or inappropriate content.
- Attempt to bypass filtering, monitoring or security arrangements.

- Share passwords or access another person's account without authorisation.
- Send abusive, discriminatory, threatening or inappropriate messages.
- Create, share or distribute harmful, manipulated or AI-generated images.
- Use unapproved AI tools or online services for school purposes.
- Upload confidential or identifiable pupil information to unapproved platforms.
- Record, photograph or share images of pupils without appropriate authorisation.
- Download unauthorised software or introduce security risks.
- Use school systems in a manner that breaches safeguarding, data protection or staff conduct requirements.

The school may monitor the use of school-managed systems and networks in accordance with its safeguarding, cybersecurity and data protection responsibilities.

Any suspected misuse must be reported promptly to the DSL, designated senior leader or IT technician, depending on the nature of the concern.

Detailed expectations are provided in the relevant acceptable use agreements.

10. Pupils using mobile devices in school

St Paul's Catholic Primary School operates as a mobile-phone-free environment throughout the school day.

Year 5 and 6 pupils may bring a mobile phone to school only where this is necessary for travel arrangements and has been agreed with the school.

Mobile phones must be switched off and handed to a designated member of staff on arrival. They will be stored securely and returned at the end of the school day.

Pupils must not access mobile phones:

- During lessons.
- Between lessons.
- During breaktimes.
- During lunchtimes.
- During school trips or activities unless specifically authorised.
- During breakfast or after-school provision unless specifically authorised by the responsible member of staff.

Smartwatches and other personal devices capable of messaging, recording, photographing, accessing the internet or sharing a location are subject to the same restrictions where their use creates safeguarding concerns.

Any unauthorised use of a mobile phone or connected device will be managed in accordance with the school's behaviour and safeguarding policies.

11. Staff using work devices outside school

Staff must take appropriate steps to protect school-managed devices and information when working outside school.

Staff must:

- Follow the school's information security, acceptable use and data protection requirements.
- Protect devices using the authentication arrangements approved by the school or its IT technician.
- Use multi-factor authentication where required.
- Lock devices when they are unattended.
- Keep devices physically secure and avoid leaving them visible in vehicles or public places.
- Ensure that family members and other unauthorised individuals do not use school devices.
- Install updates and security protections as directed by the school's IT technician.
- Use only approved platforms and applications for school work.
- Avoid accessing sensitive information over insecure public networks unless appropriate protections are in place.
- Follow school requirements when using cloud-based services or generative artificial intelligence.
- Report lost devices, suspected security breaches or unauthorised access immediately.

School-managed devices remain subject to relevant school filtering, monitoring and cybersecurity arrangements when used away from school, where technically applicable.

Concerns about device security must be reported to a member of the senior leadership team.

12. How the school will respond to issues of misuse

The school will respond promptly and proportionately to misuse of technology, school devices, networks or online platforms.

Where a concern relates to a pupil, the school will consider whether the incident should be managed through:

- The behaviour policy.
- The anti-bullying policy.
- The child protection and safeguarding policy.
- Data protection procedures.
- A combination of these arrangements.

The response will consider the pupil's age, understanding, individual needs, intent, level of risk and any wider safeguarding concerns.

Incidents involving bullying, exploitation, harassment, discriminatory behaviour, manipulated images, AI-generated content or inappropriate sexual material will be referred to the DSL.

Where a staff member, volunteer or contractor misuses school systems or personal devices in a way that raises a safeguarding or conduct concern, the matter will be managed in accordance with the staff code of conduct, safeguarding procedures and disciplinary arrangements.

The school will consider whether serious incidents should be referred to children's social care, the police, the local authority designated officer or other relevant agencies.

Safeguarding incidents and actions taken will be recorded on CPOMS.

The DSL will review incidents to identify patterns, emerging risks, training needs and any necessary changes to the curriculum or filtering and monitoring arrangements.

13. Training

All staff will receive safeguarding and online safety training as part of their induction.

All staff, including those who do not work directly with children, must read Part One of the current edition of *Keeping Children Safe in Education*.

Any Department for Education overview or summary is supplementary and does not replace the requirement to read Part One.

Online safety training will cover:

- The school's online safety and safeguarding policies.
- The four categories of online risk: content, contact, conduct and commerce.
- Filtering and monitoring arrangements and staff responsibilities.
- How to identify, record and report online safety concerns.
- The role of the DSL and deputy DSLs.
- Cyberbullying and discriminatory online behaviour.
- Online grooming, exploitation and radicalisation.
- Harmful sexual behaviour and online sexual harassment.
- Misogyny, racism and harmful online influences.
- Appropriate responses to nude and semi-nude images.
- AI-generated content, manipulated images, impersonation and chatbot risks.
- Privacy, data protection and cybersecurity.
- Additional vulnerabilities experienced by pupils with SEND.
- Emerging online risks relevant to the school community.

Staff training will be refreshed at least annually and updated when significant safeguarding risks, technologies or statutory expectations change.

The DSL and deputy DSLs will undertake appropriate safeguarding training, including online safety, at least every two years and update their knowledge and skills at regular intervals, and at least annually.

Governors will receive training appropriate to their strategic responsibilities for safeguarding, online safety, filtering and monitoring.

Supply staff, trainee teachers, volunteers and contractors will receive appropriate information or training relevant to their roles.

Staff understanding will be checked through induction records, safeguarding updates, professional discussion and review of incident reporting.

14. Monitoring arrangements

The DSL will maintain oversight of online safety concerns and ensure that incidents are recorded appropriately on CPOMS.

Online safety incidents will be reviewed to identify:

- Recurring concerns or emerging patterns.
- Pupils who may require additional support.
- Curriculum or staff training needs.
- Weaknesses in filtering, monitoring or technical arrangements.
- Opportunities to strengthen communication with parents and carers.

This policy will be reviewed at least annually and updated sooner if:

- Statutory guidance changes.
- Significant online safety incidents occur.
- New technologies are introduced.
- Filtering or monitoring arrangements change.
- Emerging risks require additional safeguards.

The annual review will include consideration of the school's online safety risk assessment and the documented annual review of filtering and monitoring provision.

The governing board will receive the revised policy and appropriate assurance regarding the effectiveness of the school's online safety arrangements.

The school's child protection and safeguarding policy will also be reviewed to ensure that online safety and filtering and monitoring responsibilities are reflected consistently.

APPENDIX 1: (SCHOOL ADMISSION PACK)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS IN EYFS AND KS1

<table>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When I use the school's IT systems (like computers/IPads) and get onto the internet in school I will:
Ask a teacher or adult if I can do so before using them
Only use websites that a teacher or adult has told me or allowed me to use
Tell my teacher immediately if:
I click on a website by mistake
I receive messages from people I don't know
I find anything that may upset or harm me or my friends
Use school computers for school work only
Be kind to others and not upset or be rude to them
Look after the school IT 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 hardest to remember my username and password
Never share my password with anyone, including my friends.
Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
Save my work on the school network
Check with my teacher before I print anything
Log off or shut down a computer when I have finished using it
I will tell a trusted adult if something online makes me worried, upset or confused.
I will stop using a website, game or device if an adult tells me to.
I understand that some pictures, videos or voices online might not be real.
I will not take photographs or make recordings without permission.
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school's IT 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 IT systems and internet, and will make sure my child understands these. I understand that the school uses appropriate filtering and monitoring arrangements and will support my child in following the school's online safety expectations.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

APPENDIX 2: (FOR TRANSITION INTO YEAR 3)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS OF CHILDREN IN KS2

Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy When I use the school's IT systems (like computers) and get onto the internet in school I will: Always use the school's IT 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 passwords 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 Always log off or shut down a computer when I'm finished working on it I will not: Access any inappropriate websites including: 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 Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate Log in to the school's network using someone else's details 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 give it to my teacher for safe keeping and 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 or other inappropriate material or use inappropriate language when communicating online 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/carer's agreement: I agree that my child can use the school's IT 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 IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	Date:

APPENDIX 3: (to be added to induction pack)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS

Name of staff member/governor/volunteers	
When using the school's IT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) Use them in any way which could harm the school's reputation Access social networking sites or chat rooms Use any improper language when communicating online, including in emails or other messaging services Install any unauthorised software, or connect unauthorised hardware or devices to the school's network Share my password with others or log in to the school's network using someone else's details Take photographs of pupils without checking with teachers first Share confidential information about the school, its pupils or staff, or other members of the community Access, modify or share data I'm not authorised to access, modify or share Promote private businesses, unless that business is directly related to the school	
I will only use the school's IT 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 IT 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 IT manager know if a pupil informs me they have found any material which 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 IT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer):	Date: