



BITTERNE
C of E PRIMARY

Online Safety Policy

Headteacher: Mrs. Jen Johnson

Reviewed by	Headteacher	Authorised by	Governing Body
Date	July 2026	Next Review	July 2027
Review Cycle	Annually	Signed by Chair of Governors	Reverend Tony Palmer

HOPE



COURAGE



CREATIVITY



Together we soar...



Version	Date	Author/Reviewed By	Summary of Changes
1.0	July 2024	Headteacher	Policy approved and adopted.
2.0	July 2026	Headteacher and DSL	Policy updated to reflect Keeping Children Safe in Education 2025, the Online Safety Act 2023, DfE Filtering and Monitoring Standards, current guidance on Artificial Intelligence (AI), cyber security and emerging online risks. References added to the Mobile Phone Policy and AI Policy. Wording reviewed and updated throughout.

Contents

Section

1. Aims
2. Legislation and Guidance
3. Roles and Responsibilities
 - 3.1 The Governing Board
 - 3.2 The Headteacher
 - 3.3 The Designated Safeguarding Lead (DSL)
 - 3.4 IT Service Provider
 - 3.5 The Data Protection Officer (DPO)
 - 3.6 All Staff and Volunteers
 - 3.7 Parents and Carers
 - 3.8 Visitors and Members of the Community
4. Educating Pupils About Online Safety
5. Educating Parents and Carers About Online Safety
6. Cyber-bullying
 - 6.1 Definition
 - 6.2 Preventing and Responding to Cyber-bullying
 - 6.3 Examining Electronic Devices
 - 6.4 Artificial Intelligence (AI)
7. Acceptable Use of the Internet in School
8. Pupils Using Mobile Devices in School
9. Staff Using Work Devices Outside School
10. Responding to Online Safety Incidents and Misuse
11. Training
12. Monitoring Arrangements
13. Links with Other Policies
- Appendix 1 – EYFS and KS1 Acceptable Use Agreement
- Appendix 2 – KS2 Acceptable Use Agreement
- Appendix 3 – Staff, Governor, Volunteer and Visitor Acceptable Use Agreement
- Appendix 4 – Online Safety Training Self-Audit
- Appendix 5 – Online Safety Incident Log



1. Aims

At Bitterne Church of England Primary School, we recognise that technology plays an essential role in children's education and everyday lives. We are committed to creating a safe, inclusive and supportive environment where pupils can benefit from technology whilst understanding how to use it safely, responsibly and respectfully.

Our school aims to:

- have robust processes in place to safeguard pupils, staff, volunteers and governors when using technology;
- identify and support pupils who may be at greater risk of online harm than others;
- provide an effective whole-school approach to online safety that enables the entire school community to use technology safely and responsibly, including computers, tablets, mobile devices and emerging technologies;
- educate pupils to become responsible digital citizens who understand how to protect themselves and others online;
- establish clear procedures to identify, respond to, record and, where appropriate, escalate online safety concerns;
- work in partnership with parents and carers to promote safe and positive use of technology beyond the school day.

The four categories of online risk

Our approach to online safety is based upon the four categories of risk identified by the Department for Education.

Content – being exposed to illegal, inappropriate or harmful content, including pornography, violent material, fake news, misinformation, disinformation, racism, misogyny, antisemitism, extremist content, conspiracy theories, self-harm and suicide content.

Contact – being subjected to harmful online interaction with other users, including bullying, peer pressure, grooming, child sexual exploitation, criminal exploitation, financial exploitation and adults posing as children or young people.

Conduct – personal online behaviour that increases the likelihood of harm, including cyberbullying, sharing personal information, sharing or creating inappropriate images, the sharing of nude and semi-nude images, online harassment and the misuse of artificial intelligence (AI).

Commerce – risks relating to online gambling, phishing, scams, financial fraud, malicious software, subscription traps and inappropriate advertising.

Online safety is recognised as an integral part of safeguarding and is embedded throughout the curriculum and wider life of the school.

2. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance Keeping Children Safe in Education (KCSIE 2025) and should be read alongside the school's Child Protection and Safeguarding Policy.

It also reflects current Department for Education guidance, including:

- Teaching Online Safety in Schools
- Relationships Education, Relationships and Sex Education (RSE) and Health Education
- Searching, Screening and Confiscation
- Sharing Nude and Semi-Nude Images: Advice for Education Settings
- Meeting Digital and Technology Standards in Schools



- DfE Filtering and Monitoring Standards
- Prevent Duty Guidance

This policy also reflects relevant legislation, including but not limited to:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011
- Equality Act 2010
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Online Safety Act 2023

The school also has regard to guidance produced by the UK Council for Internet Safety (UKCIS), the National Cyber Security Centre (NCSC), CEOP Education and the UK Safer Internet Centre where appropriate.

This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Mobile Phone Policy
- Artificial Intelligence (AI) Policy
- Data Protection Policy
- Acceptable Use Agreements

3. Roles and Responsibilities

Online safety is a whole-school responsibility. All members of the school community have an important role to play in promoting safe, responsible and respectful use of technology and in safeguarding children from online harm.

3.1 The Governing Board

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

The Governing Board will ensure that:

- the school meets its statutory safeguarding duties in relation to online safety;
- online safety remains an integral part of the school's safeguarding culture;
- appropriate filtering and monitoring systems are in place on school devices and networks and are reviewed at least annually against the Department for Education's Filtering and Monitoring Standards;
- the effectiveness of filtering and monitoring arrangements is reviewed regularly with school leaders and the school's IT provider;
- all staff receive online safety training as part of safeguarding induction and regular safeguarding updates;
- pupils receive an age-appropriate online safety curriculum;
- online safety is considered when reviewing safeguarding, behaviour and curriculum policies;
- adequate resources are available to support effective online safety arrangements.

All governors will:

- read and understand this policy;
- comply with the Staff, Governor and Visitor Acceptable Use Agreement;
- complete safeguarding and online safety training appropriate to their role;
- understand the school's filtering and monitoring arrangements;



- promote a culture of safeguarding and responsible technology use.

3.2 The Headteacher

The Headteacher is responsible for ensuring that this policy is implemented consistently across the school.

The Headteacher will:

- promote a whole-school culture of online safety;
- ensure online safety is embedded within safeguarding, teaching and learning;
- ensure staff understand their safeguarding responsibilities in relation to technology;
- work closely with the Designated Safeguarding Lead (DSL), governors and the school's IT provider to maintain effective online safety arrangements;
- ensure that online safety incidents are managed appropriately;
- ensure that the school's Mobile Phone Policy and AI Policy are implemented consistently alongside this policy.

3.3 The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety within the school.

The DSL will:

- support the Headteacher in implementing this policy;
- work with governors and the school's IT provider to review filtering and monitoring arrangements;
- oversee the management of online safety incidents and ensure they are recorded appropriately;
- ensure concerns relating to cyberbullying, online abuse, harmful sexual behaviour, the sharing of nude or semi-nude images, exploitation and emerging online risks are managed in accordance with the Child Protection and Safeguarding Policy;
- provide advice and support to staff;
- arrange appropriate staff training and updates;
- liaise with external agencies where necessary;
- provide regular reports to the Headteacher and Governing Board;
- undertake an annual online safety risk assessment to reflect current and emerging risks.

3.4 The IT Service Provider

Springwell IT provides technical support for the school's ICT systems.

Working in partnership with school leaders, Springwell IT will:

- Maintain secure school networks and devices in alignment with the DfE Cyber Security Standards for Schools.
- Implement appropriate filtering and monitoring systems, ensuring they are active on all school-owned devices.
- Enforce Multi-Factor Authentication (MFA) for all administrative accounts, staff emails, and systems containing sensitive pupil data.
- Establish, regularly test, and maintain a robust backup and recovery strategy to protect school systems from ransomware and cyber attacks.
- Implement a regular patching schedule to ensure operating systems, software, and firewalls are fully updated against emerging vulnerabilities.
- Block access to harmful or inappropriate online content and provide technical advice regarding cyber security threats.
- Safeguarding decisions remain the responsibility of school leaders.

3.5 The Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the school's data protection strategy and ensuring compliance with the UK GDPR and Data Protection Act 2018.



The DPO will:

- work alongside the DSL and Headteacher to ensure filtering and monitoring arrangements comply with data protection legislation;
- advise on Data Protection Impact Assessments (DPIAs) for new technologies, including AI tools, cloud services and educational applications;
- support the school in responding to personal data breaches arising from cyber security or online safety incidents.

3.6 All Staff and Volunteers

All staff, including supply staff, contractors and volunteers, have a responsibility to safeguard children and promote safe use of technology.

All staff will:

- read and follow this policy;
- comply with the school's Acceptable Use Agreement;
- maintain professional standards when using technology;
- follow the Staff Code of Conduct;
- follow the Mobile Phone Policy and AI Policy;
- model safe and respectful online behaviour;
- report concerns immediately to the DSL;
- understand that safeguarding incidents may occur both inside and outside school;
- participate in safeguarding and online safety training.
- Staff should only use approved school platforms for communication with pupils and parents.
- When using AI to support planning or administration, staff must follow the school's AI Policy and ensure that confidential, personal or identifiable information is not entered into AI systems unless explicitly authorised and compliant with data protection requirements.

3.7 Parents and Carers

Parents and carers play an essential role in supporting children's online safety.

The school will work in partnership with families by:

- providing information about current online risks;
- sharing guidance through newsletters, ClassDojo, the school website and meetings where appropriate;
- promoting positive digital habits.
- Parents and carers are expected to:
- support their child in following the school's Acceptable Use Agreement;
- report concerns promptly to school;
- reinforce safe and respectful online behaviour at home;
- support the school's Mobile Phone Policy where applicable.

3.8 Visitors and Members of the Community

Visitors, volunteers and members of the community using the school's ICT systems will be expected to:

- follow this policy where appropriate;
- comply with the Staff, Governor and Visitor Acceptable Use Agreement;
- follow the Mobile Phone Policy whilst on site;
- report safeguarding concerns immediately to a member of staff.

4. Educating Pupils About Online Safety

Online safety is embedded throughout the curriculum and wider school life. Pupils are taught to use technology safely, responsibly and respectfully and to recognise when they may be at risk online.

Teaching also aims to develop pupils' digital resilience so they can make informed, safe and responsible choices when using technology both now and in the future.



The school recognises that online safety is an essential part of safeguarding and is taught through the Computing curriculum, Relationships Education, PSHE, Collective Worship and other curriculum areas where appropriate.

Teaching is progressive, age-appropriate and reflects the needs of our pupils. Lessons are adapted where necessary to meet the needs of vulnerable pupils and those with SEND, recognising that some children may require additional support to understand and manage online risks.

The school uses current Department for Education guidance and appropriate educational resources to support the teaching of online safety.

All primary schools are required to teach Relationships Education and Health Education. Online safety is also taught through the National Curriculum for Computing.

In Key Stage 1, pupils will be taught to:

- use technology safely and respectfully;
- keep personal information private;
- recognise trusted adults who can help them if something online worries or upsets them;
- understand that not everything online is true;
- know how to report concerns about online content or contact.

In Key Stage 2, pupils will be taught to:

- use technology safely, responsibly and respectfully;
- recognise acceptable and unacceptable online behaviour;
- understand how to keep personal information secure;
- identify a range of ways to report online concerns;
- understand that people online may not always be who they say they are;
- make safe choices when communicating and sharing information online.

By the end of primary school, pupils will know:

- that the same values of kindness, honesty and respect apply both online and offline;
- that online actions can have real-life consequences;
- how to recognise harmful, inappropriate or misleading online content;
- how to think critically about information they find online;
- that images, videos and information generated using artificial intelligence (AI) may not always be genuine or accurate;
- how personal information is collected, shared and used online;
- what to do if they experience or witness online bullying or other harmful online behaviour;
- how and when to seek help from a trusted adult.

Online safety education is reviewed regularly to ensure it reflects current technology, emerging online risks and the needs of our pupils.

Where appropriate, online safety messages are reinforced through assemblies, themed events such as **Safer Internet Day**, classroom discussions and wider curriculum opportunities.

5. Educating Parents and Carers About Online Safety

The school recognises that parents and carers play a vital role in helping children use technology safely and responsibly. We are committed to working in partnership with families to promote positive online behaviours and to help children stay safe beyond the school day.



The school will raise parents' and carers' awareness of online safety through regular communication, including newsletters, the school website, ClassDojo, parent information sessions and other appropriate communications. This policy will also be published on the school website.

Where appropriate, the school will provide parents and carers with information about:

- current online safety risks and emerging technologies;
- age-appropriate use of social media, gaming platforms and messaging services;
- parental controls and privacy settings;
- reporting concerns about online abuse, cyberbullying or harmful content;
- promoting healthy screen time and positive digital wellbeing;
- the safe use of artificial intelligence (AI) and emerging technologies.

Parents and carers will also be informed:

- of the digital platforms and online resources used to support learning;
- where pupils may be asked to access online learning resources at home;
- of the school's expectations regarding acceptable use of technology;
- of the school's Mobile Phone Policy where this applies to their child.

The school encourages parents and carers to:

- talk regularly with their child about their online experiences;
- supervise their child's online activity in an age-appropriate way;
- encourage respectful and responsible online behaviour;
- report any online safety concerns to the school promptly so that appropriate support can be provided.

If parents or carers have concerns regarding online safety or this policy, they should contact the Designated Safeguarding Lead (DSL) or the Headteacher in the first instance.

The school may also signpost parents and carers to trusted sources of advice and guidance, including:

- UK Safer Internet Centre
- Childnet
- CEOP Education
- NSPCC
- Internet Matters

Working together with parents and carers helps ensure that pupils receive consistent messages about staying safe online both at school and at home.

6. Cyber-Bullying

6.1 Definition

Cyber-bullying is bullying that takes place using technology, including mobile phones, tablets, computers, gaming platforms, social media, messaging services and other online platforms. Like all forms of bullying, it is behaviour that is intentional, repeated and designed to cause harm or distress where there is an imbalance of power.

Cyber-bullying may include:

- sending threatening or abusive messages;
- sharing rumours or false information;
- excluding others from online groups;
- sharing photographs or videos without permission;
- impersonating another person online;



- encouraging others to join in harmful behaviour;
- using artificial intelligence (AI) to create or share harmful, misleading or manipulated content, including deepfakes.

Cyber-bullying is taken seriously and will be managed in accordance with the school's Behaviour Policy and Child Protection and Safeguarding Policy.

6.2 Preventing and Responding to Cyber-bullying

The school aims to prevent cyber-bullying through education, positive relationships and clear expectations for behaviour online.

Pupils are taught:

- how to recognise cyber-bullying;
- how to report concerns;
- how to support others who may be experiencing online bullying;
- the importance of respectful online communication;
- that online actions have real-life consequences.

Staff will:

- respond promptly to reports of cyber-bullying;
- investigate incidents fairly and proportionately;
- record concerns where appropriate;
- involve parents and carers as necessary;
- provide appropriate support for pupils affected;
- apply sanctions in line with the Behaviour Policy where appropriate.

Where online behaviour may constitute a safeguarding concern, staff will refer the matter immediately to the Designated Safeguarding Lead (DSL).

The school recognises that harmful online behaviour may include child-on-child abuse, online sexual harassment, coercive behaviour, the sharing of inappropriate images or AI-generated harmful content. Such incidents will be managed in accordance with the Child Protection and Safeguarding Policy and current Department for Education guidance.

Where illegal activity is suspected, or there is a risk of significant harm, the school will work with the police and other relevant agencies.

6.3 Examining Electronic Devices

School staff may search, examine and, where appropriate, confiscate electronic devices in accordance with current legislation and the Department for Education's guidance **Searching, Screening and Confiscation**.

Where there are reasonable grounds to believe that a device:

- presents a risk to the safety or wellbeing of pupils or staff;
- contains evidence of a breach of school rules;
- contains evidence relating to a criminal offence; or
- contains material that may place a child at risk of harm,

authorised members of staff may examine the device in line with statutory guidance.

Any search will be conducted respectfully, proportionately and with regard to the age, understanding and needs of the pupil.



If staff believe a device contains indecent images of a child or other illegal material, they will:

- **not** deliberately view or copy the images unless there is a clear safeguarding reason to do so;
- immediately inform the Designated Safeguarding Lead;
- follow current Department for Education and UKCIS guidance;
- involve the police where appropriate.

The school will retain appropriate records of significant incidents.

The use of mobile phones and personal smart devices within school is managed through the school's **Mobile Phone Policy**, which should be read alongside this policy.

6.4 Artificial Intelligence (AI)

Artificial intelligence (AI) is increasingly used within education and everyday life. While AI can enhance learning and support staff in their professional duties, it also presents safeguarding risks.

The school recognises that AI may be used to:

- create realistic but false images, audio or video (deepfakes);
- generate harmful or misleading content;
- facilitate cyber-bullying or online abuse;
- spread misinformation or disinformation.

Pupils are taught to question online content critically and to seek help if they encounter material that concerns them.

Staff are expected to use AI responsibly and professionally, in accordance with the school's **AI Policy**. AI must not be used in ways that compromise safeguarding, confidentiality, data protection or professional judgement.

7. Acceptable Use of the Internet in School

The school recognises that digital technology plays an important role in teaching, learning and communication. We encourage its safe, responsible and effective use whilst ensuring that pupils, staff and visitors are protected from online harm.

All pupils, staff, governors, volunteers and visitors are expected to use the school's ICT systems and internet responsibly and in accordance with this policy and the relevant Acceptable Use Agreement.

Use of the school's ICT systems, internet access and digital technologies must:

- support teaching, learning or the professional duties of staff;
- promote the safety and wellbeing of all members of the school community;
- comply with safeguarding, data protection and copyright legislation;
- reflect the school's values of respect, kindness and responsibility.

The school uses filtering and monitoring systems to help safeguard pupils and staff while using school networks and devices. These systems are reviewed regularly to ensure they remain appropriate and effective in line with the Department for Education's Filtering and Monitoring Standards.

Users should be aware that:

- internet activity on school devices and networks may be monitored;
- access to inappropriate or harmful material may be blocked;
- monitoring information may be reviewed where there are safeguarding, behaviour or security concerns.



Monitoring is carried out to safeguard pupils and staff, protect the school's ICT systems and fulfil statutory safeguarding responsibilities. It is undertaken in accordance with data protection legislation and the school's Data Protection Policy.

Staff must only use approved school systems and platforms when communicating with pupils, parents and carers or when storing school information.

The use of personal mobile devices is managed through the school's Mobile Phone Policy.

The use of artificial intelligence (AI) by staff and pupils is managed through the school's Artificial Intelligence (AI) Policy. Where AI tools are used to support learning or professional practice, they must be used safely, ethically and in accordance with school expectations.

Any misuse of the school's ICT systems or internet access will be dealt with in accordance with the Behaviour Policy, Staff Code of Conduct, Child Protection and Safeguarding Policy and other relevant school policies.

Further information is contained within the Acceptable Use Agreements in Appendices 1–3.

8. Pupils Using Mobile Devices in School

Bitterne Church of England Primary School recognises that some pupils may need to bring a mobile phone or other personal smart device to school for safety or travel reasons. The use of these devices must not interfere with learning, safeguarding or the wellbeing of others.

The arrangements for pupils bringing mobile phones or personal smart devices to school are set out in the school's Mobile Phone Policy, which should be read alongside this policy.

Where pupils are permitted to bring a mobile phone into school:

- written permission should be obtained from parents or carers where required;
- devices must be handed to the designated member of staff on arrival, unless alternative arrangements have been agreed by the Headteacher;
- devices must remain switched off and securely stored throughout the school day;
- devices will be returned to pupils at the end of the school day.

Pupils must not use mobile phones, smart watches or other personal smart devices during the school day unless authorised by a member of staff for a specific educational or medical purpose.

The use of personal devices to:

- take photographs or videos;
- make audio recordings;
- access social media;
- send or receive messages;
- access inappropriate content; or
- bypass the school's safeguarding systems
- is not permitted unless expressly authorised by a member of staff.

Any misuse of a mobile phone or personal smart device will be managed in accordance with the school's Mobile Phone Policy, Behaviour Policy, Child Protection and Safeguarding Policy and this Online Safety Policy.

Where the misuse of a device raises safeguarding concerns, staff will inform the Designated Safeguarding Lead (DSL) immediately.



9. Staff Using Work Devices Outside School

The school recognises that staff may use school devices and digital systems outside the school site to support teaching, learning and the effective operation of the school. Staff are expected to use all school technology safely, professionally and in accordance with safeguarding, data protection and information security requirements.

All staff are responsible for taking reasonable steps to ensure that school devices and information remain secure at all times.

This includes, but is not limited to:

- protecting devices with secure passwords or passphrases and not sharing login credentials;
- enabling multi-factor authentication (MFA) where available;
- ensuring devices are locked when unattended;
- keeping operating systems, software and security updates up to date;
- using only approved school systems and cloud-based services to store or share school information;
- taking reasonable care to protect devices from loss, theft or damage;
- reporting any lost, stolen or compromised devices immediately to the Headteacher and Springwell IT;
- ensuring confidential information cannot be viewed by unauthorised individuals when working outside school.

School devices must only be used for legitimate school business and in accordance with the Staff Code of Conduct and Acceptable Use Agreement.

Staff must not:

- allow family members or friends to use school devices;
- download unauthorised software or applications onto school equipment;
- store confidential school information on personal devices or personal cloud storage;
- use personal email accounts to send or receive confidential school information.

Where staff use artificial intelligence (AI) to support planning, administration or other professional activities, they must do so in accordance with the school's AI Policy. Confidential, personal or identifiable information must not be entered into AI systems unless specifically authorised and compliant with data protection legislation.

Any concerns regarding the security or misuse of school devices or systems must be reported immediately to the Headteacher, the Designated Safeguarding Lead (DSL) or Springwell IT, as appropriate.

10. Responding to Online Safety Incidents and Misuse

The school takes all incidents involving the misuse of technology seriously. Responses will be proportionate, educational where appropriate, and focused on safeguarding the welfare of pupils and maintaining a safe learning environment.

Where a pupil misuses the school's ICT systems, internet access or digital technology, staff will respond in accordance with the Behaviour Policy, Child Protection and Safeguarding Policy and this Online Safety Policy. The response will take account of:

- the nature and seriousness of the incident;
- the age, understanding and needs of the pupil;
- whether the behaviour was deliberate or accidental;



- any safeguarding concerns or vulnerabilities;
- previous incidents or patterns of behaviour.

Appropriate responses may include:

- discussion with the pupil to reinforce safe and responsible online behaviour;
- temporary restriction of access to school technology or online services where appropriate;
- informing parents or carers;
- recording the incident in line with school procedures;
- applying behaviour sanctions where appropriate;
- referral to the Designated Safeguarding Lead (DSL).

Where an incident raises safeguarding concerns, including online abuse, cyberbullying, child-on-child abuse, exploitation, the sharing of nude or semi-nude images, or exposure to harmful or illegal online content, staff will report the matter immediately to the DSL. The incident will be managed in accordance with the Child Protection and Safeguarding Policy and current statutory guidance.

Where a member of staff misuses school technology, school systems or personal devices in a way that may constitute misconduct or compromise safeguarding, the matter will be managed in accordance with the Staff Code of Conduct, Disciplinary Policy and relevant safeguarding procedures.

The school will consider whether incidents involving illegal activity, serious safeguarding concerns or criminal offences should be referred to external agencies, including Children's Services, the Police or other appropriate organisations.

Where incidents involve the misuse of personal mobile devices or artificial intelligence (AI), these will also be managed in accordance with the school's Mobile Phone Policy and AI Policy.

The school recognises that online safety incidents provide valuable opportunities for learning. Where appropriate, incidents will be used to reinforce online safety education and promote positive digital citizenship.

Alternative Provision (AP) Safeguarding Where a pupil is placed with an Alternative Provision provider (off-site or via distance learning), the school remains ultimately responsible for their safeguarding. The DSL will obtain written assurance from the AP provider that appropriate filtering, monitoring, and online safety protocols are in place on the devices used by the pupil. The online safety arrangements for pupils in AP placements will be reviewed by the DSL at least half-termly.

11. Training

The school recognises that effective online safety depends upon all members of the school community understanding their safeguarding responsibilities and maintaining up-to-date knowledge of current and emerging online risks.

All new staff, including temporary, supply and agency staff, will receive online safety training as part of their safeguarding induction. This will include the safe use of technology, recognising online risks, reporting concerns and understanding their responsibilities under this policy.

All staff will receive regular safeguarding and online safety updates, including annual refresher training and additional updates where appropriate. Training will reflect current statutory guidance, emerging technologies and safeguarding risks.

Through this training, staff will understand:

- that technology is a significant factor in many safeguarding and wellbeing issues;
- that children may experience abuse both online and offline, and that the two are often linked;



- how to recognise and respond to online safety concerns;
- how to report safeguarding concerns promptly;
- the importance of professional conduct when using technology;
- their responsibilities under the school's Mobile Phone Policy and AI Policy.
- Training will also help staff understand current and emerging risks, including:
 - cyberbullying;
 - child-on-child abuse;
 - online sexual harassment;
 - exploitation and grooming;
 - radicalisation;
 - misinformation and disinformation;
 - AI-generated content, including deepfakes.

The Designated Safeguarding Lead (DSL) and Deputy DSLs will undertake safeguarding training, including online safety, in accordance with statutory requirements and will keep their knowledge and skills up to date through regular professional development.

Governors will receive appropriate safeguarding and online safety training to enable them to fulfil their strategic responsibilities and understand the school's filtering and monitoring arrangements.

Volunteers will receive safeguarding information and online safety guidance appropriate to their role.

Further information regarding safeguarding training is contained within the school's Child Protection and Safeguarding Policy.

12. Monitoring Arrangements

The school recognises that online technologies and the risks associated with them continue to develop. Online safety arrangements will therefore be reviewed regularly to ensure they remain effective and continue to safeguard pupils and staff.

The Designated Safeguarding Lead (DSL) will maintain appropriate records of online safety concerns and incidents. Where appropriate, these records will be used to identify patterns, emerging risks and any additional actions required to support pupils or improve practice.

The Headteacher and DSL will work with Springwell IT to review the effectiveness of the school's filtering and monitoring arrangements. These reviews will take place at least annually using the Department for Education's digital standards self-review tools, including the Plan Technology for Your School service where appropriate to benchmark the school's infrastructure against current national standards. More frequent reviews will occur if changes in technology, updated statutory guidance, or local trends dictate.

The Governing Board will receive appropriate information regarding online safety, including significant incidents, trends and the effectiveness of the school's filtering and monitoring arrangements, to enable governors to fulfil their safeguarding responsibilities.

This policy will be reviewed annually by the Headteacher and Designated Safeguarding Lead, or sooner if:

- there are significant changes to legislation or statutory guidance;
- new safeguarding risks emerge;
- changes are made to the school's ICT systems or digital provision;
- a significant online safety incident indicates that the policy should be updated.



Following each review, the policy will be presented to the Governing Board for approval.

The review will be informed by:

- current statutory guidance;
- the school's annual safeguarding review;
- the online safety risk assessment;
- filtering and monitoring reviews;
- feedback from staff, pupils and parents where appropriate.

The Online Safety Incident Log can be found in Appendix 5.

13. Links with Other Policies

This Online Safety Policy should be read alongside the following school policies and procedures:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Relationships, Sex and Health Education (RSHE) Policy
- Mobile Phone Policy
- AI Policy
- Data Protection Policy
- Acceptable Use Agreements
- Complaints Policy
- Searching, Screening and Confiscation procedures
-

These policies work together to ensure a consistent whole-school approach to safeguarding, responsible technology use and the promotion of positive digital citizenship.



Appendix 1 – EYFS and KS1 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET

Name of pupil: _____

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

- ask an adult before using technology if I am unsure;
- only use websites, apps and games that my teacher has chosen or approved;
- tell an adult straight away if I see or hear anything that worries, upsets or confuses me;
- be kind and respectful when using technology;
- only use my own username and password;
- keep my password secret;
- never share my personal information with anyone online unless my teacher says it is safe to do so;
- look after school equipment carefully;
- only use technology for my learning;
- ask an adult before using any AI-powered tools or apps provided by the school;
- log off or close my device when I have finished.

I understand that school may monitor how computers and the internet are used to help keep everyone safe.

Pupil Signature: _____

Date: _____

Parent/Carer Agreement

I have read this agreement with my child and will help them use technology safely and responsibly.

I understand that the school will monitor the use of school devices and internet access to safeguard pupils.

Parent/Carer Signature: _____

Date: _____



Appendix 2 – KS2 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET

Name: _____

When using school technology I will:

- use school devices and the internet safely, respectfully and responsibly;
- only use technology for learning unless a member of staff gives permission;
- keep my passwords secure;
- protect my personal information and other people's information;
- tell a trusted adult immediately if I see anything online that worries me;
- think carefully before posting, sharing or commenting online;
- remember that online actions have real-life consequences;
- use AI tools only when instructed or authorised by my teacher;
- understand that AI-generated information may not always be correct;
- follow my teacher's instructions when using online resources.

I will not:

- access inappropriate websites or material;
- deliberately bypass the school's filtering systems;
- use someone else's login details;
- share photographs or videos without permission;
- use social media, messaging services or online games unless directed by my teacher for learning;
- use AI to complete work dishonestly or present AI-generated work as entirely my own;
- bring my mobile phone or smart device into school without following the school's **Mobile Phone Policy**.

I understand that school may monitor my use of school technology to help keep everyone safe.

Pupil Signature: _____ Date: _____

Parent/Carer Agreement

I have discussed this agreement with my child and will support them in using technology safely at home and at school.

Parent/Carer Signature: _____ Date: _____



Appendix 3 – Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS

Name: _____

When using school technology, I will:

- use school systems professionally and responsibly;
- safeguard confidential information;
- follow the school's Data Protection Policy, Staff Code of Conduct, Mobile Phone Policy and AI Policy;
- use only approved school systems for storing and sharing school information;
- protect devices using secure passwords or passphrases and multi-factor authentication where available;
- report lost devices, suspected security breaches or safeguarding concerns immediately;
- ensure confidential information cannot be viewed by unauthorised people when working away from school;
- model safe and responsible online behaviour for pupils.

I will not:

- access inappropriate or illegal material;
- install unauthorised software;
- use personal email accounts to send confidential school information;
- store confidential information on personal cloud storage;
- enter confidential, personal or identifiable information into AI systems unless authorised by the school and compliant with data protection requirements;
- use AI-generated content without checking it carefully for accuracy, bias and suitability before using it professionally;
- communicate with pupils using personal social media or messaging platforms;
- share my passwords or allow others to use my school account.

I understand that my use of school technology may be monitored for safeguarding, security and operational purposes.

Signature: _____ Date: _____



Appendix 4 – Online Safety Training Self-Audit

Name _____ Date _____

Question	Yes	No
Do you know who the Designated Safeguarding Lead (DSL) is?	☐	☐
Do you understand your responsibilities for online safety?	☐	☐
Are you familiar with the school's filtering and monitoring arrangements?	☐	☐
Do you know how to report an online safety concern?	☐	☐
Are you familiar with the Acceptable Use Agreement?	☐	☐
Do you understand the school's Mobile Phone Policy?	☐	☐
Do you understand the school's Artificial Intelligence (AI) Policy?	☐	☐
Are you confident using approved digital systems securely?	☐	☐
Do you feel equipped to recognise and address the risks surrounding online misinformation, disinformation, and AI deepfakes	☐	☐
Would you benefit from additional online safety training?	☐	☐
Are you confident identifying and reporting instances of online child-on-child sexual harassment or harmful sexual behaviours?	☐	☐
Comments		



Appendix 5 – Online Safety Incident Log

Date	Location	Description of Incident	Action Taken	Recorded By