E-Safety and Acceptable Use Policy

1.0 Document Control and Policy Approval

1.1 Policy Title, Version, and Review Cycle

This document is the E-Safety and Acceptable Use Policy for [School Name]. It outlines the school's approach to safeguarding children and staff in relation to digital technologies and online activities. The current version is [Version Number], approved on [Date of Policy Approval]. The scheduled review date is [Review Date], and the policy will be reviewed at least annually, or sooner if required by changes in statutory guidance or emerging risks.

1.2 Policy Ownership and Approval

The policy is owned by [Name of Headteacher] and the Designated Safeguarding Lead ([Name of Designated Lead]). Approval is the responsibility of the Governing Body, who last approved this policy on [Date of Policy Approval]. The policy will be reviewed and updated in consultation with staff, pupils, parents/carers, and relevant external agencies.

1.3 Policy Status and Distribution

This policy is statutory and mandatory for all members of the school community, including staff, pupils, parents/carers, governors, volunteers, and visitors. It is published on the school website, available in hard copy from the school office, and distributed to all staff and governors. Key extracts and guidance are shared with parents/carers and pupils through regular communications and induction processes.

2.0 Policy Statement and Scope

2.1 Policy Statement

[School Name] is committed to safeguarding and promoting the welfare of all children and young people. We recognise the importance of robust E-Safety and acceptable use practices in protecting pupils, staff, and the wider school community from online risks and harms. Our policy reflects statutory duties under Keeping Children Safe in Education (KCSIE), the Education Act 2002, the Children Act 2004, and other relevant legislation. We strive to create a safe, supportive, and inclusive learning environment where digital technologies are used responsibly and confidently.

2.2 Purpose and Aims

The purpose of this policy is to set out clear expectations, procedures, and responsibilities for safe and acceptable use of digital technologies within [School Name]. Our aims are to:

- Protect pupils, staff, and the school community from online risks, including cyberbullying, exploitation, radicalisation, and inappropriate content.
- Promote digital resilience, critical thinking, and healthy online habits.
- Ensure compliance with all relevant legal and regulatory requirements, including data protection and safeguarding obligations.
- Foster a culture of respect, responsibility, and positive digital citizenship.
- Provide clear guidance and support for responding to E-Safety incidents and concerns.

2.3 Scope of Policy

This policy applies to all members of the school community: staff (including supply and peripatetic staff), pupils, governors, volunteers, contractors, and visitors. It covers all devices (school-owned and personal), systems, networks, and online platforms used in school or for school-related activities, including remote learning environments. The policy encompasses all digital communications, including email, social media, messaging apps, and online collaboration tools.

3.0 Roles and Responsibilities

3.1 Governing Body and Leadership

The Governing Body holds strategic oversight and accountability for E-Safety and acceptable use within [School Name]. Governors ensure that robust policies and procedures are in place, regularly reviewed, and compliant with statutory requirements. They monitor the effectiveness of safeguarding arrangements, including E-Safety education, technical controls, and incident management. Governors receive regular reports on E-Safety matters and participate in policy review and evaluation processes.

3.2 Headteacher and Senior Leadership Team (SLT)

The Headteacher and SLT are responsible for the operational implementation of this policy. They ensure that all staff are aware of their responsibilities, receive appropriate training, and adhere to Acceptable Use Agreements. The SLT oversees the deployment and review of filtering and monitoring systems, ensures that E-Safety is embedded across the curriculum, and leads the response to E-Safety incidents. They work closely with the DSL to ensure effective safeguarding and compliance with statutory guidance.

3.3 Designated Safeguarding Lead (DSL) and Deputies

The DSL ([Name of Designated Lead]) and deputies are responsible for managing E-Safety incidents and concerns. They provide advice and support to staff, pupils, and parents/carers, and liaise with external agencies such as the Local Authority, CEOP, and the police when necessary. The DSL ensures that all safeguarding concerns, including those arising from online activity, are recorded, investigated, and responded to in accordance with school and statutory procedures. The DSL also leads staff training on E-Safety and keeps up to date with emerging risks and best practice.

3.4 Staff Responsibilities

All staff are expected to model safe and responsible online behaviour, adhere to Acceptable Use Agreements, and promote E-Safety within their roles. Staff must report any E-Safety concerns or incidents to the DSL immediately, using the school's reporting procedures. Staff are responsible for supervising pupils' use of digital technologies, implementing curriculum-based E-Safety education, and supporting pupils in developing digital resilience. Staff must complete mandatory E-Safety and safeguarding training, and participate in regular updates.

3.5 Pupil Responsibilities

Pupils are expected to use digital technologies safely, respectfully, and responsibly, in accordance with the school's Acceptable Use Agreements. Pupils should report any concerns, incidents, or inappropriate content to a trusted adult or the DSL. They are encouraged to participate actively in E-Safety education, ask questions, and seek help when needed. Pupils must not engage in cyberbullying, online harassment, or any behaviour that could harm themselves or others. They should respect the privacy and rights of others online.

3.6 Parent/Carer Engagement

Parents and carers play a vital role in supporting E-Safety and acceptable use. The school provides regular information, guidance, and opportunities for engagement, including workshops, newsletters, and online resources. Parents/carers are expected to discuss E-Safety with their children, reinforce safe online behaviours, and sign Acceptable Use Agreements. The school encourages parents/carers to report concerns and seek advice from the DSL or school staff.

3.7 Technical Support/ICT Team

The ICT team is responsible for maintaining secure and reliable digital systems, implementing robust filtering and monitoring controls, and responding promptly to technical incidents. They ensure that all devices and networks comply with data protection and safeguarding requirements, and support staff and pupils in safe use of technology. The ICT team regularly reviews technical standards, updates systems in line with DfE and NCSC guidance, and provides technical advice to the SLT and DSL.

4.0 Policy Implementation

4.1 Acceptable Use Agreements (AUA)

Acceptable Use Agreements are developed for staff, pupils, and visitors, tailored to age and role. These agreements set out clear expectations for safe and responsible use of school systems, devices, and online platforms. AUAs are distributed during induction, reviewed annually, and updated in response to emerging risks. Signed consent is obtained and recorded for all staff and pupils; parents/carers sign on behalf of younger pupils. AUAs are accessible, written in clear language, and reinforced through ongoing education and reminders.

4.2 E-Safety Education and Curriculum Integration

E-Safety is embedded across the curriculum, including computing, PSHE, and assemblies. The school uses the UKCIS Education for a Connected World framework, CEOP Thinkuknow resources, and scenario-based learning to build digital resilience and critical thinking. E-Safety topics are age-appropriate and progressive, covering online risks, digital wellbeing, cyberbullying, privacy, and safe use of social media. Pupils are encouraged to reflect on their online experiences, discuss dilemmas, and develop strategies for staying safe.

4.3 Staff Training and Professional Development

All staff receive mandatory induction training on E-Safety and safeguarding, including statutory guidance and school procedures. Ongoing professional development is provided through regular updates, workshops, and online modules. Training covers emerging risks, technical controls, incident management, and curriculum integration. Staff are supported in developing confidence and expertise in teaching E-Safety and responding to online concerns. The DSL and ICT team provide specialist advice and support as needed.

4.4 Parental Engagement and Communication

The school actively engages parents/carers in E-Safety through a range of strategies. Regular workshops and information sessions are held to share best practice, discuss current risks, and answer questions. Newsletters, guidance leaflets, and online resources are provided to support parents/carers in reinforcing safe behaviours at home. The school encourages open dialogue, invites feedback, and responds promptly to parental concerns. Parents/carers are involved in policy review and consultation processes.

5.0 Technical Controls and Safeguarding Measures

5.1 Filtering and Monitoring Systems

[School Name] implements robust filtering and monitoring systems to protect pupils and staff from inappropriate content, online harms, and security threats. Systems are regularly reviewed and updated in line with DfE and NCSC guidance, ensuring age-appropriate access and effective alerts. The ICT team monitors usage, investigates alerts, and reports concerns to the DSL. Procedures are in place for responding to breaches, technical incidents, and requests for access to blocked content (subject to safeguarding review).

5.2 Device and Network Security

Protocols are established for the secure use of school-owned and personal devices (BYOD), including password protection, encryption, and regular updates. Remote learning platforms are configured to safeguard privacy and restrict unauthorised access. Staff and pupils are trained in secure practices, such as logging out, reporting lost devices, and avoiding risky downloads. The ICT team conducts regular audits, updates security software, and responds to technical incidents promptly.

5.3 Data Protection and Privacy

The school complies with the Data Protection Act 2018 and UK GDPR, ensuring the safe handling of personal data and digital images. Staff are trained in data protection principles, including consent, confidentiality, and secure storage. Procedures are in place for managing data breaches, responding to subject access requests, and protecting sensitive information. Pupils and parents/carers are informed about privacy rights and how their data is used. Digital images and recordings are only used with appropriate consent and for educational purposes.

6.0 Online Behaviour, Digital Wellbeing, and Safeguarding

6.1 Promoting Positive Online Behaviour

[School Name] promotes respectful, responsible, and safe online conduct for all members of the school community. Pupils and staff are expected to treat others with kindness, avoid cyberbullying and harassment, and respect the privacy and rights of others. The school provides education and guidance on digital etiquette, responsible communication, and the consequences of negative behaviour. Positive role modelling, peer support, and restorative approaches are used to reinforce expectations.

6.2 Addressing Online Risks and Harms

The school recognises a range of online risks, including cyberbullying, online sexual harassment, radicalisation, exploitation, scams, and misinformation. Procedures are in place for identifying, preventing, and responding to these risks. Staff are trained to recognise signs of online harm, intervene appropriately, and escalate concerns to the DSL. Pupils are taught how to recognise risks, seek help, and protect themselves and others. The school works with external agencies, such as CEOP and the Local Authority, to support pupils at risk.

6.3 Supporting Digital Wellbeing and Mental Health

Digital wellbeing is a key priority for [School Name]. The school promotes healthy online habits, balance between screen time and other activities, and strategies for managing stress and anxiety related to online experiences. Pupils are encouraged to reflect on their online activity, discuss challenges, and seek support when needed. Staff are trained to recognise the impact of online activity on mental health and provide appropriate guidance and referrals. The school signposts pupils and parents/carers to external support services and resources.

7.0 Incident Management and Reporting

7.1 Reporting E-Safety Concerns and Incidents

Clear procedures are in place for reporting E-Safety concerns and incidents. Staff, pupils, and parents/carers are encouraged to report concerns promptly to the DSL or a trusted member of staff. Reporting can be done verbally, via email, or using the E-Safety Incident Report Form (see Appendix 10.2). All safeguarding concerns must be reported to the DSL immediately, who will assess the risk and take appropriate action, including referral to external agencies where necessary.

7.2 Responding to E-Safety Incidents

The school follows a structured process for investigating, recording, and responding to E-Safety incidents. The DSL leads the response, supported by the SLT and ICT team as required. Actions may include safeguarding interventions, disciplinary measures, support for those affected, and engagement with external agencies. The school ensures that all incidents are handled sensitively, confidentially, and in accordance with statutory guidance. Lessons learned from incidents are used to inform policy review and staff training.

7.3 Record Keeping and Documentation

Accurate records are maintained for all E-Safety incidents, concerns, and actions taken. Records are stored securely, in line with data protection requirements, and accessible only to authorised staff. Documentation includes incident details, investigation outcomes, support provided, and referrals made. The DSL is responsible for maintaining the E-Safety incident log and reporting trends to the Governing Body. Records are reviewed regularly to identify patterns and inform preventative measures.

7.4 Whistleblowing and Confidentiality

The school's Whistleblowing Policy and safeguarding protocols protect those who report E-Safety concerns. Staff, pupils, and parents/carers are assured of confidentiality and support when raising concerns. The school does not tolerate victimisation or retaliation against whistleblowers. All reports are handled in accordance with statutory guidance and school procedures, with appropriate protection for those involved.

8.0 Policy Review, Monitoring, and Evaluation

8.1 Policy Review Cycle and Process

This policy is reviewed at least annually, or sooner if required by changes in legislation, statutory guidance, or emerging risks. The review process involves consultation with staff, pupils, parents/carers, governors, and relevant external agencies. Feedback is sought through surveys, meetings, and incident analysis. Updates are communicated to all stakeholders, and training is provided on new procedures.

8.2 Monitoring and Compliance

The school monitors the implementation of this policy through regular audits, compliance checks, and evaluation of E-Safety education. The SLT and Governing Body receive reports on policy effectiveness, incident trends, and training outcomes. Surveys and feedback from pupils, staff, and parents/carers are used to assess understanding and engagement. The school takes prompt action to address gaps or weaknesses identified through monitoring.

8.3 Responding to Regulatory Changes

Procedures are in place for updating the policy in response to changes in legislation, statutory guidance, or inspection frameworks. The DSL and SLT monitor updates from the DfE, Ofsted, UKCIS, and other relevant bodies, and ensure that policy and practice remain compliant. Significant changes are communicated to all stakeholders, and training is provided as needed.

9.0 Linked Policies and Related Documents

This policy should be read in conjunction with other relevant school policies, including:

- Safeguarding and Child Protection Policy: Procedures for protecting pupils from harm, including online risks.
- Behaviour Policy: Expectations for conduct, including online behaviour and consequences for breaches.
- Anti-Bullying Policy: Strategies for preventing and responding to bullying, including cyberbullying.
- Data Protection Policy: Procedures for handling personal data and ensuring privacy.
- Whistleblowing Policy: Protection for those reporting concerns.
- Remote Learning Policy: Guidelines for safe and effective online teaching and learning.
- Staff Code of Conduct: Expectations for professional behaviour, including online interactions.

10.0 Appendices

10.1 Model Acceptable Use Agreements (Staff, Pupils, Visitors)

Templates for Acceptable Use Agreements are provided for staff, pupils (by age group), and visitors. These agreements set out clear expectations for safe and responsible use of school systems, devices, and online platforms. Consent forms are included for parents/carers of younger pupils. Agreements are reviewed annually and updated as needed.

[Insert Model Acceptable Use Agreements and Consent Forms here]

10.2 E-Safety Incident Report Form

A standardised form is provided for recording and reporting E-Safety incidents. The form includes sections for incident details, actions taken, and outcomes. Staff, pupils, and parents/carers can use the form to report concerns to the DSL.

[Insert E-Safety Incident Report Form template here]

10.3 E-Safety Curriculum Overview

An overview of E-Safety education is provided, outlining progression across year groups and curriculum areas. The overview references statutory frameworks (DfE, UKCIS) and best practice resources (CEOP, Thinkuknow).

[Insert E-Safety Curriculum Overview here]

10.4 Parental Guidance and Resources

Sample communications, guidance leaflets, and links to recommended resources are included to support parents/carers in reinforcing E-Safety at home. Resources include UKCIS, CEOP, Thinkuknow, and National Cyber Security Centre guidance.

[Insert Parental Guidance Leaflets and Resource Links here]

10.5 Filtering and Monitoring Technical Standards Checklist

A checklist is provided for reviewing technical controls in line with DfE and NCSC guidance. The checklist covers filtering, monitoring, device security, and incident response.

[Insert Filtering and Monitoring Standards Checklist here]

11.0 References

- Keeping Children Safe in Education (KCSIE) 2025
- The Education Act 2002
- The Children Act 2004
- Data Protection Act 2018 and UK GDPR
- Prevent Duty (Counter-Terrorism and Security Act 2015)
- Working Together to Safeguard Children
- DfE: Teaching Online Safety in Schools
- DfE Filtering and Monitoring Standards
- UKCIS Education for a Connected World
- Ofsted Inspection Framework
- SWGfL 360 Degree Safe Tool
- CEOP/Thinkuknow Resources

- National Cyber Security Centre (NCSC) Guidance
- Online Safety Act (as relevant)
- [Local Authority Name] Safeguarding Partnership Guidance