Orchard Community Primary School

ONLINE SAFETY POLICY

Policy owner	Headteacher / IT Manager / Computing Lead / Designated Safeguarding Lead
Approved by	Governing Body
Version	2.0
Effective from	September 2026, reviewed & updated by KS
Review date	September 2029

Contents

- 1. Purpose and aims
- 2. Scope
- 3. Legislation and statutory guidance
- 4. Whole-school approach and principles
- 5. Roles and responsibilities
- 6. Teaching pupils about online safety
- 7. Online safety curriculum content and progression
- 8. Staff training and professional use
- 9. Parent and carer engagement
- 10. Filtering and monitoring
- 11. Cyber security, data protection and information security
- 12. Artificial intelligence and emerging technologies
- 13. Mobile phones and personal devices
- 14. Online communication, email and social media
- 15. Online bullying and child-on-child abuse
- 16. Responding to online safety incidents
- 17. Searching, screening, confiscation and evidence
- 18. Remote and off-site use of school technology
- 19. Accessibility, inclusion and additional needs
- 20. Acceptable use
- 21. Links with other policies
- 22. Monitoring, review and governance
- Appendix 1: Key online safety messages for pupils
- Appendix 2: Useful sources and support

1. Purpose and aims

Orchard Community Primary School is committed to creating a safe, positive and inclusive digital environment in which pupils can benefit from technology while being protected from avoidable harm. Online safety is part of safeguarding and is the responsibility of everyone in the school community.

This policy updates the school's previous E-Safety Policy and uses the current term 'online safety' throughout. It should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour Policy, Acceptable Use Policy and Data Protection arrangements.

The school aims to:

- protect pupils, staff, volunteers, governors and visitors from online risks and abuse;
- educate pupils to use technology safely, respectfully, responsibly and critically;
- support pupils to recognise risk, make safer choices and seek help when something online worries them;
- promote positive, age-appropriate use of digital technology rather than presenting technology as inherently negative;
- ensure staff understand their safeguarding responsibilities when using technology and responding to online concerns;
- maintain appropriate filtering, monitoring and cyber security arrangements;
- work openly with parents and carers to support safe and healthy digital use at home;
- ensure online safety is inclusive and responsive to pupils' age, maturity, SEND, communication needs and individual risk.

2. Scope

This policy applies to all pupils, staff, governors, volunteers, contractors, agency staff, visitors and anyone else who uses or accesses the school's networks, devices, accounts or digital services. It applies whether technology is used on school premises, on school trips, during remote learning, or through school-owned equipment used away from school.

The school recognises that online harm can occur outside school and outside school hours. Where an incident affects the safety, wellbeing or education of a pupil, the school will respond in line with safeguarding, behaviour and other relevant procedures.

3. Legislation and statutory guidance

This policy is informed by current statutory guidance and relevant legislation applicable to schools in England, including:

- Keeping Children Safe in Education 2026 (KCSIE), in force from 1 September 2026;
- Working Together to Safeguard Children 2026 and associated safeguarding arrangements;
- Department for Education filtering and monitoring standards for schools and colleges;
- Department for Education cyber security standards for schools and colleges;
- Department for Education guidance on meeting digital and technology standards in schools and colleges;
- Department for Education guidance on Mobile phones in schools, which became statutory from 29 June 2026 and is to be followed from 1 September 2026;
- Department for Education guidance on data protection in schools;
- Department for Education guidance and training on the safe use of generative AI in education;
- Prevent duty guidance, where relevant to online radicalisation and extremist content;
- Education Acts and regulations relating to safeguarding, behaviour, searching and confiscation;
- Equality Act 2010 and the school's duties to make reasonable adjustments and promote equality;
- UK GDPR and the Data Protection Act 2018, as amended by relevant current legislation;
- Online Safety Act 2023, where relevant to understanding the wider online environment and platform responsibilities.

The school will review this policy when statutory guidance or other significant requirements change. The most recent version of KCSIE and relevant DfE guidance will take precedence where there is any conflict.

The school does not rely on filtering and monitoring as a substitute for teaching, supervision, professional judgement or safeguarding procedures.

4. Whole-school approach and principles

KCSIE identifies online safety as an important part of a whole-school safeguarding approach. Orchard Community Primary School therefore treats online safety as a running and interrelated theme across safeguarding, curriculum, staff training, parental engagement, filtering and monitoring, behaviour, data protection and digital technology governance.

The school considers the four areas of online risk commonly described as the 4Cs: content, contact, conduct and commerce. The school also considers emerging risks including AI-generated content, deepfakes, scams, phishing, harmful online communities, gaming-related risks, inappropriate advertising and the sharing of personal information.

Online safety education will be age-appropriate, developmentally appropriate and inclusive. Pupils will be supported to develop digital resilience, critical thinking and the confidence to ask for help.

5. Roles and responsibilities

5.1 Governing Body

- Ensure that online safety is reflected in the school's safeguarding arrangements and relevant policies.
- Hold leaders to account for the effectiveness of online safety arrangements.
- Ensure appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least annually.
- Receive appropriate assurance about filtering, monitoring, cyber security, online incidents and actions taken.
- Ensure staff have appropriate safeguarding training and understand their responsibilities.

5.2 Headteacher and Senior Leadership Team

- Ensure this policy is implemented consistently and reviewed appropriately.
- Ensure online safety is integrated into safeguarding, curriculum, staff development and parental engagement.
- Ensure appropriate action is taken when online safety concerns arise.
- Ensure serious incidents are escalated to the DSL, governors and external agencies where appropriate.

5.3 Designated Safeguarding Lead

- Lead on safeguarding aspects of online safety and ensure online concerns are managed through the school's safeguarding procedures.
- Respond to concerns identified through filtering and monitoring.
- Ensure online safety incidents and safeguarding concerns are recorded appropriately.
- Work with IT support, senior leaders and governors to review filtering and monitoring.
- Consider referrals to children's social care, police or other agencies where appropriate.
- Ensure staff know how to report online safety concerns.

5.4 Computing Lead / Online Safety Lead

- Coordinate online safety education and resources across the school.
- Provide regular updates.
- Work with the DSL and IT support to identify emerging online risks.
- Support pupil voice and Digital Leaders where appropriate.
- Coordinate parent information and signposting.

5.5 IT Network Manager / IT Support

- Maintain appropriate filtering and monitoring systems and provide reports or alerts to authorised staff.
- Maintain appropriate cyber security controls, system updates, malware protection, access controls and backups.
- Ensure school devices and accounts are managed securely.
- Investigate technical incidents and escalate safeguarding concerns to the DSL.
- Support annual filtering and monitoring reviews and record technical checks.

5.6 All staff, volunteers and contractors

- Read and follow this policy and the school's safeguarding and acceptable use arrangements.
- Complete required online safety and safeguarding training.
- Use school technology professionally and securely.
- Report concerns promptly to the DSL and/or appropriate IT support.
- Never assume that an online concern is 'just an IT issue' where safeguarding may be involved.

5.7 Pupils

- Use technology safely, respectfully and responsibly.
- Follow the school's acceptable use expectations.
- Tell a trusted adult if something online worries, frightens or confuses them.
- Respect other people's privacy, property, images and personal information.

5.8 Parents and carers

- Work with the school to support safe and responsible use of technology.
- Raise concerns promptly with the school where online activity may affect a child's safety or wellbeing.
- Support children to follow age restrictions, privacy settings and appropriate family rules.

6. Teaching pupils about online safety

Online safety is taught explicitly and reinforced through the wider curriculum, safeguarding work, PSHE/RSE, assemblies, computing and everyday classroom practice. In EYFS, where computing is not taught as a separate subject, online safety is woven into learning, routines and discussions in an age-appropriate way. The school also participates in Safer Internet Day and uses other opportunities to reinforce safe digital behaviours.

Teaching will help pupils understand that online safety is not only about avoiding harmful content. It also involves relationships, behaviour, privacy, information, money, advertising, wellbeing and making informed choices.

Pupils will be taught how to report concerns and how to seek help from trusted adults. Reporting routes will be revisited regularly.

7. Online safety curriculum content and progression

EYFS

- Begin to recognise that technology is used by people in everyday life.
- Begin to understand that some things should be kept private.
- Begin to recognise safe and unsafe situations and identify trusted adults who can help.
- Use age-appropriate language and stories to explore kindness, asking for help and safe choices.
- Develop early awareness that not everything seen or heard through technology is suitable or true.

Key Stage 1

- Use technology safely, respectfully and responsibly.
- Keep personal information private and understand why passwords and personal details matter.
- Recognise that people may communicate differently online.
- Identify trusted adults and ways to report concerns about content or contact.
- Understand basic risks from games, apps, advertising and sharing information.
- Begin to recognise that online information may be inaccurate or misleading.

Key Stage 2

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour online.
- Understand the 4Cs and identify risks relating to content, contact, conduct and commerce.
- Understand how information and data are collected, shared and used.
- Critically evaluate online information, images, videos and sources.
- Understand age ratings, privacy settings, reporting tools and blocking functions.
- Recognise risks associated with people they have never met and understand appropriate responses.

- Understand online bullying, peer-on-peer abuse, harmful content and how to seek help.
- Develop awareness of scams, phishing, online financial risks and persuasive advertising.
- Develop age-appropriate understanding of AI, including generated images, videos and text, misinformation, privacy and the need to check information.

Curriculum planning should reflect pupils' needs and the school's current risk profile. Online safety teaching will be adapted for pupils with SEND, communication needs or other vulnerabilities.

8. Staff training and professional use

All new staff will receive online safety information as part of induction and will be required to understand the school's acceptable use and safeguarding arrangements. Online safety will be included in safeguarding updates and annual training, with additional updates provided when significant risks, systems or guidance change.

- Staff will be made aware of current online harms and emerging risks relevant to children.
- Staff will understand how filtering and monitoring works in the school and how to report concerns.
- Staff will understand the safeguarding, data protection and intellectual property risks associated with generative AI.
- Staff will not enter confidential or personal pupil information into unapproved AI tools or online services.
- Staff will use school-approved accounts, systems and platforms for professional communication.
- Personal social media use must not compromise professional boundaries, confidentiality or the school's reputation.

9. Parent and carer engagement

The school recognises parents and carers as key partners in online safety. Information will be shared through the school website, newsletters, parent meetings, digital communications and other appropriate channels.

- The school will provide practical, positive guidance on helping children use technology safely.
- Parents and carers will be signposted to reliable sources of support and reporting.
- The school will communicate about age ratings, parental controls, emerging apps and games, scams and relevant online risks where appropriate.
- Parents will be encouraged to discuss online experiences with their children and establish clear, age-appropriate family expectations.
- Concerns raised by parents will be considered through safeguarding, behaviour and online safety procedures as appropriate.

The school will continue to promote reliable sources such as Childline, CEOP, the UK Safer Internet Centre, Internet Matters, the NSPCC and DfE resources.

10. Filtering and monitoring

The school will maintain appropriate filtering and monitoring systems to provide a safe digital environment. Filtering is preventative: it aims to block illegal, inappropriate and potentially harmful content. Monitoring is reactive: it identifies activity that may require investigation and does not itself prevent access.

Filtering and monitoring will be managed as part of safeguarding, not solely as an IT function.

- The DSL will lead on safeguarding aspects, including reviewing relevant alerts and responding to concerns.
- IT support will maintain systems, provide technical reports and investigate technical issues.
- Senior leaders, the DSL, IT support and the responsible governor will review filtering and monitoring effectiveness at least annually.
- The annual review will consider the school's pupil risk profile, including age, SEND, EAL, vulnerabilities, digital resilience and emerging risks.
- Reviews will consider whether filtering and monitoring cover school-owned devices, off-site use and relevant applications and services.
- The school will consider the ability of its systems to address dynamic, personalised and AI-generated content.
- Checks will be documented, including actions required and evidence of completion.
- Filtering will not unreasonably restrict legitimate teaching and learning.
- No filtering system is 100% effective. Staff supervision, education and professional judgement remain essential.

The school's current monitoring arrangements use SENSO on Windows and Chromebook devices and the SENSO app where applicable on iPads, subject to technical limitations and supplier changes. The school will review this provision as part of its annual filtering and monitoring review.

11. Cyber security, data protection and information security

Cyber security is part of safeguarding because a cyber incident can compromise systems and sensitive information relating to children and staff. The school will work towards the Department for Education's cyber security standards and maintain proportionate technical and organisational measures.

- Use strong, unique passwords and multi-factor authentication where available and appropriate.
- Limit user access to the systems and information required for a person's role.
- Keep devices, operating systems, applications and security software appropriately updated.
- Use anti-malware and firewall protections and maintain appropriate backups.
- Report suspected phishing, malware, lost devices, compromised accounts or other cyber incidents immediately.
- Do not share passwords or allow unauthorised people to use school accounts.
- Protect confidential information when working away from school.
- Use approved systems for storing and transferring personal data.
- Complete appropriate data protection impact assessments before introducing high-risk new systems or significant changes to monitoring or processing.
- Follow the school's privacy notices and data protection procedures.

Filtering and monitoring data will be accessed only by authorised staff, retained appropriately and handled in accordance with data protection requirements.

12. Artificial intelligence and emerging technologies

The school recognises that generative AI is increasingly part of children's and adults' digital environment. AI may provide educational benefits but can also create safeguarding, privacy, accuracy, bias, intellectual property and wellbeing risks.

- Any AI tool used in school must be approved through the school's technology, safeguarding and data protection arrangements.
- Staff must not input confidential, sensitive or personally identifiable pupil information into unapproved AI services.
- Where AI-generated content is used, staff remain responsible for checking accuracy, appropriateness, bias and suitability.
- Pupils will be taught age-appropriate critical thinking about AI, including that AI-generated material can be inaccurate or misleading and that images, audio and video can be manipulated.
- The school will consider AI-generated content when reviewing filtering and monitoring provision.
- The school will consider the DfE's Generative AI: product safety standards when assessing products.
- Use of AI must support, rather than replace, professional judgement, safeguarding and meaningful teaching and learning.

13. Mobile phones and personal devices

From 1 September 2026, the school will follow the Department for Education's statutory guidance Mobile phones in schools. The school will operate a mobile-phone-free environment by default, subject only to clearly defined exceptions where necessary.

- Pupils must follow the school's mobile phone arrangements during the whole school day, including lessons, breaktimes and lunchtime.
- Where pupils bring mobile phones or other personal devices to school, they must be stored securely in accordance with the school's arrangements.
- Any approved exception must be authorised by the school and managed safely.
- Personal devices must not be used to photograph, record or share pupils or staff without appropriate permission.
- Where a device is misused, the school will respond in accordance with behaviour, safeguarding and acceptable use procedures.

14. Online communication, email and social media

- Pupils and staff will use school-approved accounts and platforms for school-related communication.
- Pupil email use will be supervised and monitored where appropriate.
- Staff will maintain professional boundaries and will not use personal messaging services to communicate privately with pupils unless specifically authorised under a school-approved system.
- School communications will comply with data protection, confidentiality and safeguarding requirements.
- Staff must not post confidential information, images or comments about pupils or colleagues on personal social media.
- Suspicious emails, attachments, links or requests for information must be reported rather than opened or forwarded.

15. Online bullying and child-on-child abuse

The school recognises that bullying and child-on-child abuse can occur through messaging, social media, gaming, image sharing and other online environments. Online abuse will not be dismissed as 'banter' or normal behaviour.

- Pupils will be taught how to recognise and report online bullying and harmful behaviour.
- Reports will be taken seriously and considered through safeguarding and behaviour procedures.
- The school will consider the impact on all children involved, including victims, alleged perpetrators and witnesses.
- Online sexual harassment, sharing of intimate images, coercion, grooming, threats, hate incidents and other harmful behaviour will be managed as safeguarding concerns.
- Where a child may be at risk of significant harm, the DSL will follow the school's safeguarding referral procedures.
- The school may work with parents, children's social care, police or other agencies where appropriate.

16. Responding to online safety incidents

Any online safety concern should be reported promptly. Staff should not investigate beyond what is necessary to establish immediate safety or preserve information safely unless authorised to do so.

The response will depend on the nature and seriousness of the incident and may include:

- immediate safeguarding action;
- reporting to the DSL or deputy DSL;
- technical investigation by IT support;
- recording on the appropriate safeguarding, behaviour or online safety system;
- contact with parents/carers where appropriate;
- support for the pupil or staff member affected;
- action under the Behaviour Policy, Acceptable Use Policy or staff procedures;
- referral to children's social care, police, CEOP or another agency where appropriate;
- review of filtering, monitoring, curriculum or staff training following significant incidents.

Accidental access to inappropriate content should be reported and recorded. Staff and pupils should not deliberately search for, download, copy or distribute harmful or illegal content.

17. Searching, screening, confiscation and evidence

The school will follow current DfE guidance on searching, screening and confiscation and the school's Behaviour Policy. Where a device may contain safeguarding evidence, staff will act proportionately, preserve evidence where appropriate and seek advice from the DSL and senior leaders.

The school will consider the legal and safeguarding implications before accessing or copying personal content from a device. Where illegal material or a serious safeguarding concern may be involved, the school will seek appropriate advice and consider referral to the police or other relevant agency.

18. Remote and off-site use of school technology

School-owned devices and accounts remain subject to this policy when used away from school. Staff and pupils must protect devices, accounts and information and report loss, theft or suspected compromise immediately.

- School devices must be secured from unauthorised access.
- Staff must not allow family members or other unauthorised people to use school devices or accounts.
- School data must only be stored or transferred through approved systems.
- Online learning or communication with pupils must use school-approved platforms and professional boundaries.
- Safeguarding concerns arising from remote or off-site activity must be reported through normal safeguarding procedures.

19. Accessibility, inclusion and additional needs

The school recognises that online safety risks and protective factors vary between pupils. Online safety education and support will be adapted to meet individual needs, including SEND, communication difficulties, neurodiversity, EAL, vulnerabilities and differing levels of digital experience.

- Teaching will use accessible language, visuals, modelling and repetition where appropriate.
- Individual risk assessments or support plans may include specific online safety arrangements.
- Filtering and monitoring reviews will consider the needs of pupils with SEND and other vulnerabilities.
- The school will balance safeguarding with appropriate access to technology and assistive tools.
- Pupils will be supported to develop independence and digital resilience at an appropriate level.

20. Acceptable use

All pupils, staff, governors, volunteers and relevant visitors will follow the school's Acceptable Use Policy. Acceptable use arrangements will be age-appropriate and will cover school devices, accounts, networks, online services and relevant personal devices.

- Use technology for agreed educational or professional purposes.
- Respect privacy, confidentiality, copyright and intellectual property.
- Do not access, create, store or share illegal, discriminatory, abusive or harmful content.
- Do not attempt to bypass security, filtering or monitoring systems.
- Do not use another person's account or credentials.
- Report concerns, mistakes, inappropriate content or security incidents promptly.
- Understand that school systems may be filtered and monitored for safeguarding and security purposes.

21. Links with other policies

This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Acceptable Use Policy
- Data Protection Policy and Privacy Notices
- Staff Code of Conduct and disciplinary procedures
- Social Media Policy, where applicable
- Computing Policy
- AI Policy / guidance, where applicable
- Complaints Procedure
- Mobile Phone arrangements
- Cyber Security arrangements and incident response procedures

22. Monitoring, review and governance

The policy will be reviewed at least annually and sooner if there are significant changes to legislation, KCSIE, DfE guidance, technology, school systems or the school's risk profile.

- The DSL, Computing Lead, Headteacher and IT support will contribute to the review.
- The responsible governor will receive appropriate assurance about implementation.
- Filtering and monitoring effectiveness will be formally reviewed and documented at least annually.
- Online safety incidents and trends will inform curriculum planning, staff training and parental engagement.

- Significant incidents will be reviewed to identify lessons and necessary changes.
- The governing body will be informed of significant online safety risks and actions.

Appendix 1: Key online safety messages for pupils

Messages will be adapted to age and need, but pupils should increasingly understand that:

- Tell a trusted adult if something online makes you feel worried, frightened, uncomfortable or confused.
- Be kind and respectful online. Online behaviour can affect people just as much as behaviour face-to-face.
- Keep personal information private and use passwords safely.
- Do not assume everyone online is who they say they are.
- Not everything online is true. Check information and ask for help when unsure.
- Do not share pictures or videos of other people without permission.
- Use reporting and blocking tools when appropriate.
- Think before clicking links, downloading files or giving information.
- If you make a mistake online, tell a trusted adult. Getting help early is important.
- AI-generated images, videos, audio and text can look real but may not be true.

Appendix 2: Useful sources and support

Source	Purpose
Department for Education	Keeping Children Safe in Education 2026; Mobile phones in schools; filtering and monitoring; cyber security; data protection; AI guidance.
UK Safer Internet Centre	Resources, advice and reporting information for schools, children and families.
Child Exploitation and Online Protection (CEOP)	Reporting and support relating to online sexual abuse and exploitation.
Childline	Confidential advice and support for children and young people.
Internet Matters	Practical parent and carer guidance about children's online lives.
NSPCC	Safeguarding and online safety advice for families and professionals.
National Cyber Security Centre	Cyber security guidance and advice for schools and organisations.

Key reference documents used for this update

- Department for Education, Keeping children safe in education 2026, statutory guidance, in force from 1 September 2026.
- Department for Education, Meeting digital and technology standards in schools and colleges – Filtering and monitoring: core standard, updated 16 September 2026.
- Department for Education, Meeting digital and technology standards in schools and colleges – Cyber security: core standard, updated 16 September 2026.
- Department for Education, Mobile phones in schools, statutory guidance, updated 29 June 2026; guidance applies from 1 September 2026.
- Department for Education, Data protection in schools, updated 9 July 2026.
- Department for Education, Generative AI: product safety standards, updated 19 January 2026.
- Department for Education, Safe use of generative AI in education: module 3, updated 19 May 2026.

This policy should be read with the school's current safeguarding and operational procedures. Where a statutory requirement or newer official guidance is published after this policy, leaders should review and amend the policy as necessary rather than waiting for the scheduled annual review.