ONLINE SAFETY POLICY

Larkfield Primary School

KCSIE 2026 aligned version

School	Larkfield Primary School
Policy owner	Designated Safeguarding Lead (DSL) / Headteacher Jan Flynn/Dave Palmen
Approved by	Governing Body
Approval date	
Effective from	September 2026
Review date	September 2027 – at least annually
Version	1.0 – KCSIE 2026

Document status: *This policy is intended to be adopted and then completed with the school's local safeguarding contacts, technical arrangements, filtering/monitoring provider, acceptable use arrangements and related policy names. It should be read alongside the school's Child Protection and Safeguarding Policy.*

Contents

1. Policy statement and purpose
2. Scope
3. Legal and statutory framework
4. Aims and objectives
5. Understanding online safety risks – the 4Cs
6. Roles and responsibilities
7. Curriculum and preventative education
8. Filtering and monitoring
9. Online safety incident response and reporting
10. Cyberbullying, harmful online behaviour and child-on-child abuse
11. Sexual imagery, nudes and semi-nudes, including AI-generated content
12. Generative artificial intelligence (AI)
13. Devices, accounts, passwords and information security
14. Mobile phones and personal devices
15. Staff professional use of technology
16. Remote learning and online communication
17. Data protection, privacy and digital consent
18. Inclusion and pupils who may be more vulnerable
19. Parents and carers
20. Staff and governor training
21. Monitoring, evaluation and assurance
22. Breaches and consequences
23. Policy review
Appendix 1 – School online safety contacts and reporting routes
Appendix 2 – Filtering and monitoring annual review record
Appendix 3 – Online safety incident response checklist
Appendix 4 – Related policies and documents
Appendix 5 – KCSIE 2026 / DfE compliance checklist

1. Policy statement and purpose

This Online Safety Policy sets out how Larkfield Primary will protect and educate pupils, staff and other members of the school community in their use of digital technology. It forms part of the school's wider safeguarding arrangements and should be read alongside the Child Protection and Safeguarding Policy.

The school recognises that technology is integral to learning, communication and everyday life. Online safety is therefore treated as a continuing safeguarding responsibility rather than a standalone Computing issue.

The policy is based on the school's existing online safety guidance and has been updated to reflect the statutory and departmental requirements in force from September 2026, including Keeping Children Safe in Education 2026 (KCSIE 2026), the Department for Education filtering and monitoring standard, current cyber-security expectations, and the 2026 statutory position on mobile phones in schools.

The school will take a child-centred, proportionate and preventative approach. It will seek to empower pupils with the knowledge, skills and confidence to make safe choices while maintaining appropriate technical controls, supervision and reporting arrangements.

2. Scope

This policy applies to all pupils, staff, governors, volunteers, visitors, contractors and other users of school technology or school networks, whether on or off the school premises.

- school-owned computers, laptops, tablets, interactive displays and other connected devices;
- school networks, wireless networks, cloud services, learning platforms and school-managed accounts;
- school-approved websites, apps, online learning platforms and digital services;
- personal devices where they are brought onto or used within the school environment or to access school systems;
- remote learning, virtual meetings and online communication undertaken on behalf of the school; and
- generative AI tools and other emerging technologies where they are used for teaching, learning, administration or communication.

3. Legal and statutory framework

This policy should be implemented in conjunction with the school's wider safeguarding and data protection arrangements. The principal framework considered in this version is:

- Keeping Children Safe in Education 2026 (DfE), in force from 1 September 2026;
- Teaching online safety in schools (DfE);
- Education for a Connected World (UK Council for Internet Safety);
- Department for Education Filtering and Monitoring: core standard;
- Department for Education Generative AI: product safety standards / expectations and related guidance;
- Mobile phones in schools (DfE), statutory from 29 June 2026 and to be implemented by schools from 1 September 2026;
- Searching, Screening and Confiscation (DfE);
- Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025;
- relevant Prevent duty guidance and safeguarding guidance;
- Department for Education digital and technology standards, including cyber security; and
- other current statutory guidance and local safeguarding partnership procedures relevant to the school.

The school will review this policy whenever relevant statutory guidance changes and at least annually.

4. Aims and objectives

The school aims to:

- protect pupils from potentially harmful and inappropriate online material and interactions;
- teach pupils to use technology safely, responsibly and respectfully;
- develop critical thinking, digital literacy and resilience so pupils can recognise and manage online risks;
- ensure online safety is taught progressively from Reception through Year 6 and reinforced across the curriculum;
- provide appropriate filtering and monitoring and ensure these systems are reviewed at least annually;
- ensure staff understand their safeguarding responsibilities in relation to online safety, filtering and monitoring;
- provide clear, accessible reporting routes for pupils, staff and parents/carers;
- respond promptly and proportionately to online safety concerns and incidents;
- support pupils who may be more vulnerable to online harm, including pupils with SEND and other additional needs;
- work with parents and carers to promote safe and healthy use of technology beyond school; and
- protect personal information and maintain secure systems through appropriate cyber-security and data-protection measures.

5. Understanding online safety risks – the 4Cs

The school uses the four areas of risk identified in KCSIE 2026 as a framework for teaching, prevention, filtering, monitoring and safeguarding response.

Risk area	Examples relevant to primary pupils
Content	Exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation and conspiracy theories.
Contact	Harmful interactions with others, including peer pressure, grooming, adults posing as children, exploitation, targeted advertising and harmful interactions with or through generative AI.
Conduct	Unsafe or harmful online behaviour, including cyberbullying, sharing explicit material, non-consensual sharing, harmful challenges, abusive messages and AI-generated harmful imagery.
Commerce	Online gambling, scams, phishing, inappropriate advertising, financial scams, manipulative commercial content and unsafe in-app purchasing.

The school recognises that online harms may occur alongside offline safeguarding concerns. Staff must therefore consider the wider safeguarding context and report concerns through the school's safeguarding procedures.

6. Roles and responsibilities

6.1 Governing body / Trust Board

- Provide strategic oversight and assurance that online safety is embedded within safeguarding.
- Ensure appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least once every academic year.
- Receive assurance on the annual filtering and monitoring review, identified gaps and actions taken.
- Ensure appropriate resources, training and governance arrangements are available.
- Ensure this policy is reviewed and aligned with other safeguarding and technology policies.

6.2 Headteacher

- Provide overall leadership for the school's online safety culture.
- Ensure the policy is implemented consistently.
- Approve arrangements for temporary exceptions to filtering/monitoring where necessary and ensure they are documented.
- Ensure serious incidents are managed in line with safeguarding, behaviour, disciplinary and legal requirements.

6.3 Designated Safeguarding Lead (DSL)

- Have day-to-day responsibility for online safety within the safeguarding framework.
- Ensure online safety concerns identified through filtering, monitoring, pupil reports or staff reports are appropriately assessed and escalated.
- Maintain or oversee records of safeguarding-related online incidents and identify trends.
- Work with IT support to understand alerts, reporting and system limitations.
- Ensure online safety is reflected in safeguarding training, curriculum planning and parental engagement.
- Provide advice to staff and liaise with external agencies where required.

6.4 IT / Network Manager or IT provider (APEX)

- Maintain and monitor technical systems in accordance with agreed responsibilities.
- Ensure filtering and monitoring are active, appropriately configured and applied to relevant devices and users.
- Provide clear reporting and urgent escalation of high-risk technical or safeguarding alerts.
- Support annual review and technical testing, including checks following significant system changes.
- Support cyber-security, account management, updates and secure configuration.

6.5 Computing / Online Safety Lead

- Coordinate the progressive online safety curriculum.
- Support staff with age-appropriate resources and emerging online risks.
- Work with the DSL to ensure curriculum concerns are referred through safeguarding procedures.

6.6 All staff

- Model safe, respectful and responsible use of technology.
- Supervise pupils appropriately when they use devices.
- Follow the school's acceptable use requirements.
- Complete required safeguarding and online safety training.
- Report online safety concerns promptly to the DSL or through the school's agreed reporting route.
- Understand that filtering and monitoring do not replace professional supervision.

6.7 Pupils

- Use technology in accordance with the school's age-appropriate acceptable use expectations.
- Treat others respectfully online and offline.
- Protect passwords and personal information.
- Tell a trusted adult if something online makes them worried, uncomfortable or unsafe.
- Do not deliberately bypass filtering or monitoring or use another person's account.

6.8 Parents and carers

- Support the school's online safety expectations.
- Supervise and discuss children's online activity in an age-appropriate way.
- Raise concerns with the school where online activity may affect a child's safety or wellbeing.
- Follow school arrangements for the use of personal devices and online communication.

7. Curriculum and preventative education

Online safety is embedded throughout the curriculum, with explicit teaching through Computing, PSHE/RSE and other appropriate curriculum areas. The school may use Purple Mash 2BeSafe or another approved scheme, alongside resources from DfE, UKCIS, CEOP Education, Childnet and other reputable providers.

- Teaching will be age- and developmentally appropriate and will build progressively from Reception to Year 6.
- Lessons will address content, contact, conduct and commerce risks.
- Pupils will be taught how to recognise unreliable information, misinformation, manipulation, advertising and other persuasive techniques.
- Pupils will be taught how to report concerns and how to seek help from trusted adults.
- Online safety will be reinforced through assemblies, wider curriculum opportunities, classroom routines, displays, pupil voice and staff role modelling.
- Teaching will take account of emerging risks, including AI-generated content and harmful online challenges.
- External speakers and online safety resources will be checked for suitability, safeguarding and age appropriateness.
- Staff will respond to safeguarding disclosures made during online safety teaching in accordance with the Child Protection and Safeguarding Policy.

8. Filtering and monitoring

The school will maintain appropriate filtering and monitoring systems to reduce pupils' exposure to illegal, inappropriate and potentially harmful content. Filtering is preventative; monitoring is reactive and may generate alerts or reports for activity that requires review.

8.1 Annual review

The governing body/proprietor will ensure that the effectiveness of filtering and monitoring is reviewed at least once every academic year. The review will be led by the SLT member responsible for filtering and monitoring, with the DSL and IT support, and will provide assurance to the governing body/trust board.

The review will include checks that filtering is working appropriately on all relevant internet-connected devices and in relevant locations, and a record of checks and actions will be retained.

8.2 What the review will consider

- age range and risk profile of pupils;
- SEND, EAL and other relevant vulnerabilities;
- school-managed devices and any approved BYOD arrangements;
- all locations and relevant off-site use;
- what content the system blocks and allows and whether this remains appropriate;
- whether harmful and inappropriate content is blocked without unreasonable impact on teaching and learning;
- safe-search arrangements and technical controls;
- monitoring coverage, alerts and incident-response arrangements;
- whether users can be identified where necessary;
- new technologies and generative AI tools;
- technical limitations and any gaps in protection;
- recent safeguarding incidents and trends;
- staff understanding and training;
- temporary exceptions and whether these have been appropriately authorised and recorded; and
- whether changes to hardware, software or network configuration have affected filtering or monitoring.

8.3 Monitoring arrangements

- All staff will provide appropriate in-person supervision when pupils use devices.
- Where technical monitoring is used, it will generate alerts/reports appropriate to the school's risk profile.
- High-risk alerts will be escalated promptly to the DSL and/or relevant IT lead.
- Weekly monitoring reports will be reviewed where this is supported by the school's monitoring solution and will include action/outcome recording for significant incidents.
- Monitoring procedures will identify who receives alerts, who acts, expected timescales and how actions are recorded.
- Users will be informed that school devices and networks are subject to filtering and monitoring.
- Monitoring arrangements will be reflected in relevant acceptable use and privacy information.
- Where technical monitoring involves personal data, the school will maintain appropriate data protection documentation, including a DPIA where required.

8.4 Limitations and exceptions

The school recognises that no filtering system is 100% effective. Staff remain responsible for appropriate supervision and professional judgement. Any temporary exception to filtering or monitoring must be authorised by the appropriate SLT lead, documented, time-limited and risk assessed.

9. Online safety incident response and reporting

Any concern that a child may be at risk of harm online must be treated as a safeguarding concern and reported through the school's established safeguarding route – CPOMs.

9.1 Pupils

- Tell a trusted adult as soon as possible.
- Where appropriate, stop interacting with the person/account causing concern.
- Do not delete evidence if this can be avoided; seek adult help before taking further action.
- Use the school's reporting mechanism where one is provided.

9.2 Staff

- Listen and take the concern seriously.
- Do not promise confidentiality.
- Record relevant facts accurately and promptly.
- Report to the DSL/deputy DSL without delay.
- Do not independently investigate beyond what is necessary to establish immediate safety.
- Where technical evidence or device activity is relevant, involve IT support through the agreed process.

9.3 DSL response

- Assess immediate safeguarding risk and follow the Child Protection and Safeguarding Policy.
- Consider whether the concern involves abuse, exploitation, child-on-child abuse, sexual harassment/violence, criminal exploitation, radicalisation, self-harm or another safeguarding category.
- Decide whether referral to children's social care, police, CEOP or another agency is required.
- Ensure appropriate records are made and information is shared on a need-to-know basis.
- Work with IT support where technical evidence or system changes are required.
- Review whether the incident indicates a weakness in curriculum, supervision, filtering, monitoring, staff training or policy.

10. Cyberbullying, harmful online behaviour and child-on-child Abuse

Cyberbullying and other harmful online behaviour will be treated as safeguarding and/or behaviour concerns as appropriate. The school recognises that child-on-child abuse can occur online and may include abusive or harassing messages, misogynistic or misandrist messages, sharing pornography with someone who does not want to receive it, and the non-consensual creation or sharing of nudes or semi-nudes.

- Reports will be taken seriously and assessed individually.
- The school will support the child reporting or experiencing harm and will consider the needs of all children involved.
- Behaviour consequences will be proportionate and consistent with the Behaviour Policy.
- Where the behaviour may constitute a safeguarding concern or criminal offence, the DSL will consider appropriate external referral.
- Evidence will be handled sensitively and in line with safeguarding and data protection requirements.

11. Sexual imagery, nudes and semi-nudes, including AI-generated content

The school will follow current UKCIS and DfE guidance when responding to the making or sharing of nudes and semi-nudes. KCSIE 2026 recognises that such images may be photographs, videos, livestreams, digitally altered images or wholly AI-generated content, including deepfakes or deep nudes.

- Staff must not view, copy, download or distribute sexual images of children except where specifically permitted by law and current safeguarding guidance.
- Any disclosure or discovery must be reported promptly to the DSL/deputy DSL.
- The DSL will follow the school's safeguarding procedures and current specialist guidance, including consideration of police/CEOP referral where appropriate.
- Children will be treated with dignity and supported without shame or blame.
- Where AI-generated imagery is involved, the school will consider both the safeguarding harm and the technology used to create or distribute the material.

12. Generative artificial intelligence (AI)

The school recognises that generative AI creates educational opportunities but also introduces safeguarding, privacy, misinformation, intellectual property and inappropriate-content risks.

- Only school-approved AI tools may be used by pupils or staff for school purposes.
- Before adopting an AI product, the school will assess safeguarding, privacy, data protection, age appropriateness, content moderation and procurement requirements.
- Where a product processes personal data, the school will consider data protection requirements and complete a DPIA where required.
- Staff must not enter confidential or personal pupil information into an AI tool unless this has been explicitly approved through the school's data protection arrangements.
- Pupil-facing AI tools must be age appropriate and configured to minimise harmful content and unsafe interactions.
- AI-generated content must be checked by an adult before it is used in teaching or sent to families where accuracy, safeguarding or appropriateness could be affected.
- Pupils will be taught that AI-generated information may be inaccurate, biased or misleading and should be checked against reliable sources.
- AI-generated images or content that could harm a child, constitute abuse or amount to non-consensual sexual imagery must be treated as a safeguarding concern.

13. Devices, accounts, passwords and information security

- Each user will have an individual account where practicable. Accounts must not be shared.
- Passwords must be kept confidential and strong authentication will be used where available and proportionate.
- Devices must be locked when unattended and staff must not leave sensitive information visible.
- Software, operating systems and security controls will be kept appropriately updated.
- Users must not install unauthorised software or connect unauthorised devices to the school network.
- School data must be stored and shared using approved systems.
- Lost or stolen devices must be reported immediately.
- Suspected phishing, malware, compromised accounts or data breaches must be reported immediately through the school's agreed route.
- The school will maintain appropriate cyber-security arrangements consistent with current DfE standards and the school's risk profile.

14. Mobile phones and personal devices

From 1 September 2026, the school will operate in accordance with the DfE statutory guidance Mobile phones in schools. The school's default position is that pupils do not have access to mobile phones throughout the school day, including lessons, between lessons, breaktimes and lunchtime, except where an agreed exception applies.

The detailed arrangements, including storage, exceptional access, sanctions and searching/confiscation procedures, are set out in the school's Mobile Phone Policy and Behaviour Policy. Where a personal device is used for an approved educational or safeguarding purpose, the school will apply appropriate supervision, filtering/monitoring and data protection arrangements.

Staff personal devices must not be used to photograph, record or communicate with pupils except where explicitly authorised under school procedures.

15. Staff professional use of technology

- Staff must use school-approved systems for professional communication with pupils and families.
- Staff must maintain professional boundaries in all online communication.
- Personal social media accounts must not be used to communicate privately with pupils.
- Staff must follow the Staff Code of Conduct and acceptable use arrangements.
- Images, recordings and pupil work must be stored and shared only through approved systems.
- Staff must report accidental access to inappropriate material, inappropriate contact or concerns about another staff member's online behaviour in accordance with safeguarding and staff conduct procedures.
- Low-level concerns about staff digital behaviour will be managed in accordance with the Staff Code of Conduct and safeguarding procedures.

16. Remote learning and online communication

- Remote learning will use school-approved platforms.
- Staff will use professional accounts and approved communication channels.
- Online lessons will be appropriately supervised and recorded where the school's procedures and data protection arrangements permit or require this.
- Pupils and parents will receive clear expectations about online conduct, privacy and reporting concerns.
- Staff will consider safeguarding implications when pupils are participating from home or another location.
- Any concern arising during remote learning will be reported through the school's safeguarding procedures.

17. Data protection, privacy and digital consent

Online safety and data protection are closely connected. The school will comply with applicable data protection laws and maintain appropriate technical and organisational measures.

- Only necessary personal data will be collected and processed for legitimate school purposes.
- Staff will use approved systems for pupil information and avoid unnecessary duplication of personal data.
- Photographs and videos will be handled in accordance with the school's privacy notices, permissions and data protection procedures.
- Third-party digital services will be assessed before use, including consideration of data processing, age appropriateness, security and safeguarding.
- Technical monitoring arrangements will be transparent and reflected in relevant privacy information.
- Where required, Data Protection Impact Assessments will be completed and reviewed.

18. Inclusion and pupils who may be more vulnerable

The school recognises that all children may experience online harm, while some pupils may need additional support. This may include pupils with SEND, EAL, communication needs, care experience or other vulnerabilities.

- Online safety teaching will be adapted to pupils' communication and learning needs.
- Visual supports, modelling, repetition, simplified language and practical scenarios will be used where appropriate.
- Staff will consider whether a pupil's additional needs affect their ability to understand, recognise or report online risks.
- The SENCO, DSL and relevant pastoral staff will work together where additional support is needed.
- Technology and accessibility features will be used to reduce barriers to learning without compromising safeguarding.

19. Parents and carers

- Parents/carers will receive clear information about the school's online safety expectations.
- Acceptable Use Agreements will be shared as appropriate and reviewed regularly.
- The school will provide practical advice about apps, games, devices, parental controls, online communication and emerging risks.
- Parents will be informed when significant emerging online risks are identified that may affect pupils.
- The school will signpost families to reputable support such as Childnet, Internet Matters, UK Safer Internet Centre and CEOP Education.
- Parent feedback will inform policy review and online safety provision where appropriate.

20. Staff and governor training

- All staff will receive safeguarding and child protection training that includes online safety and an understanding of filtering and monitoring responsibilities as part of induction.
- Online safety updates will be provided at least annually and more frequently when risks, technology or guidance change.
- Training will include reporting routes, safe professional use of technology, emerging online harms, AI risks and the school's filtering and monitoring arrangements.
- The DSL/deputy DSL will maintain appropriate safeguarding knowledge and access specialist updates.
- Governors/trustees will receive appropriate information and assurance so they can fulfil their strategic safeguarding responsibilities.
- The impact of training will be considered through staff feedback, incident trends, monitoring and safeguarding review.

21. Monitoring, evaluation and assurance

The school will monitor online safety through a combination of safeguarding, curriculum, technical and stakeholder evidence.

- annual online safety policy review;
- annual filtering and monitoring effectiveness review;
- recorded checks of filtering on relevant internet-connected devices and locations;
- review of monitoring alerts and significant incidents;
- pupil voice and age-appropriate surveys;
- staff feedback and confidence checks;
- learning walks, work scrutiny and curriculum review;
- parent feedback;
- technical audits and provider assurance;
- review of acceptable use compliance;
- review of cyber-security incidents and data protection concerns; and
- governor/trustee safeguarding reporting.

Findings will be used to identify actions, allocate resources and update training, curriculum provision, technical controls and policy.

22. Breaches and consequences

Breaches of this policy will be considered in accordance with the nature of the concern and the relevant school policies.

- Pupil breaches will normally be managed under the Behaviour Policy and acceptable use arrangements, with safeguarding procedures applied where required.
- Staff breaches will be managed under the Staff Code of Conduct and Disciplinary Policy where appropriate.
- Serious or potentially criminal matters will be escalated to the DSL, Headteacher and/or relevant external agencies.
- Sanctions will be proportionate and will take account of the child's age, understanding, additional needs and safeguarding context.
- The school will use incidents as opportunities to identify learning, supervision or systems improvements.

23. Policy review

This policy will be reviewed at least annually and sooner where there are significant changes to statutory guidance, technology, local safeguarding risks, filtering/monitoring systems or school practice.

The annual review will consider incident logs, filtering and monitoring reports, technical audits, pupil/staff/parent voice, curriculum evidence, training evaluations and relevant national/local guidance. The governing body/trust board will receive appropriate assurance about the review and any actions.

This policy will be aligned with the Child Protection and Safeguarding Policy, Behaviour Policy, Computing Policy, PSHE/RSE Policy, Staff Code of Conduct, Acceptable Use Agreements, Mobile Phone Policy, Data Protection/Privacy arrangements, Remote Learning arrangements and relevant cyber-security procedures.

Appendix 1 – School online safety contacts and reporting routes

Role / service	Named person / provider	Contact / reporting route
Designated Safeguarding Lead (DSL)	Jan Flynn	jflynn@larkfieldprimary.co.uk CPOMs
Deputy DSL	Dave Palmen Anna Felmingham	head@larkfieldprimary.co.uk afelmingham@larkfieldprimary.co.uk
Headteacher	Dave Palmen	head@larkfieldprimary.co.uk
IT / Network Manager or provider	APEX	support@apexns.co.uk
Filtering provider	Netsweeper	support@apexns.co.uk
Monitoring provider		[INSERT SUPPORT ROUTE]
Local safeguarding partnership		
Police / emergency	999 in an emergency	999 / 101 as appropriate
CEOP Education / Safety Centre	CEOP	See link on school website

Appendix 2 – Filtering and monitoring termly review record

Complete this record at least once every academic year and retain it as evidence of the review.

Review item	Evidence / action / date
Responsible SLT member identified	
DSL involved in review	
IT support/provider involved	
Responsible governor/trustee informed	
All school-managed devices checked	iPads Chromebooks PCs
Relevant internet-connected locations checked	
Filtering block/allow profile reviewed	
Safe search settings checked	
Monitoring alerts and reports reviewed	
High-risk alert process tested	
User identification arrangements checked	
Off-site / remote device arrangements checked	
BYOD arrangements reviewed (if applicable)	
Generative AI products reviewed (if applicable)	
Recent safeguarding incidents considered	
SEND/EAL/vulnerability profile considered	
Temporary exceptions reviewed	
Provider assurance / technical limitations considered	
DPIA/privacy arrangements reviewed where required	
Actions recorded, assigned and dated	
Outcome reported to governing body/trust board	

Appendix 3 – Online safety incident response checklist

- 1. Ensure the child/person is safe and identify any immediate risk.
- 2. Report to the DSL/deputy DSL promptly.
- 3. Record the concern factually using the school's safeguarding recording system.
- 4. Do not promise confidentiality.
- 5. Preserve relevant evidence without unnecessarily viewing, copying or distributing harmful material.
- 6. DSL assesses safeguarding risk and decides on escalation/referral.
- 7. IT support is involved where filtering, monitoring, account security or technical evidence is relevant.
- 8. Consider whether other pupils may be affected.
- 9. Consider whether parents/carers should be informed, taking safeguarding advice before doing so.
- 10. Record actions, decisions and outcomes.
- 11. Review whether curriculum, supervision, training, filtering, monitoring or policy changes are required.

Appendix 4 – Related policies and documents

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Disciplinary Policy
- Computing Policy
- PSHE / RSE Policy
- Mobile Phone Policy
- Acceptable Use Agreements – pupils, staff and parents/carers
- Data Protection / Privacy Notices
- Remote Learning Policy / safeguarding procedures
- Cyber Security Policy / Business Continuity arrangements
- Searching, Screening and Confiscation procedures
- Whistleblowing Policy

Appendix 5 – KCSIE 2026 / DfE compliance checklist

This checklist is a practical cross-reference for school leaders. It is not a substitute for reading the statutory guidance.

Requirement / expectation	Where addressed in this policy	School evidence / action
Online safety is part of the whole-school safeguarding approach	Sections 1, 3, 6, 21	
Four areas of online risk (content, contact, conduct, commerce) considered	Section 5	
Online safety teaching is progressive and embedded across curriculum	Section 7	
Staff safeguarding training includes online safety and filtering/monitoring responsibilities	Section 20	
Appropriate filtering and monitoring systems are in place	Section 8	
Filtering and monitoring effectiveness reviewed at least once every academic year	Section 8 / Appendix 2	
Annual review includes checks across relevant internet-connected devices/locations and records outcomes	Section 8 / Appendix 2	
Filtering balances safeguarding with access to legitimate learning content	Section 8	
Monitoring arrangements include clear alert, escalation and recording procedures	Section 8	
Users are informed that monitoring is in place	Section 8	
AI / generative AI safeguarding considerations are addressed	Section 12	
AI use is considered alongside data protection and product safety	Sections 12 and 17	
Cyber security and information security are part of safeguarding arrangements	Section 13	
Mobile phone arrangements align with statutory DfE guidance	Section 14	
Online harms may be considered alongside offline safeguarding concerns	Sections 5, 9 and 10	
Nudes/semi-nudes and AI-generated sexual imagery are addressed	Section 11	
Support is adapted for pupils with SEND/EAL and other vulnerabilities	Section 18	
Parents/carers are engaged and supported	Section 19	

Requirement / expectation	Where addressed in this policy	School evidence / action
Policy is reviewed at least annually and following significant change	Section 23	

References and source documents

The policy has been developed from the school's supplied Guidance for Online Safety Policy (2Simple) and checked against current Department for Education guidance available in September 2026.

- Department for Education (2026), Keeping children safe in education 2026: statutory guidance for schools and colleges.
- Department for Education (2026), Meeting digital and technology standards in schools and colleges – Filtering and monitoring: core standard.
- Department for Education (2026), Meeting digital and technology standards in schools and colleges – Cyber security: core standard and related standards.
- Department for Education (2026), Generative AI: product safety standards.
- Department for Education (2026), Mobile phones in schools.
- Department for Education (2026), Data protection in schools.
- UK Council for Internet Safety, Education for a Connected World.
- UK Council for Internet Safety / DfE, Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- School source document: Guidance for Online Safety Policy (2Simple), supplied by the school.

Important implementation note: *Before approval, the school should complete all bracketed local information, confirm its actual filtering/monitoring arrangements and provider, align the policy with its current Child Protection and Safeguarding Policy and Mobile Phone Policy, and ensure the named roles and reporting routes are accurate.*