Connected Futures Partnership

Authoring our story.

Dorothy Gardner Nursery School
Mary Paterson Nursery School
Tachbrook Nursery School
Essendine Primary School
Hallfield Primary School
Oxford Gardens Primary School
Queen's Park Primary School
Queen's Park Family Hub
Bayswater Children's Centre

Online Safety Policy

SEPTEMBER 2026

Table of Contents

1. Purpose and status 3
2. Scope 3
3. The four areas of online risk 3
4. Principles 3
5. Roles and responsibilities 4
6. Safeguarding and reporting concerns 4
7. Nude and semi-nude images and sexual content 5
8. Filtering and monitoring 5
9. Generative artificial intelligence (AI) 5
10. Online safety education 5
11. Staff and governor training 6
12. Parents and carers 6
13. Accounts, passwords and access 6
14. Cyber security and technical resilience 6
15. Email, messaging and communication 6
16. Online learning and collaboration platforms 7
17. Social media and professional boundaries 7
18. Mobile phones, wearable and personal devices 7
19. Images, video and audio 7
20. Data protection and privacy 7
21. Digital accessibility and inclusion 8
22. Digital images, copyright and intellectual property 8
23. Incident recording, monitoring and learning 8
24. Review of this policy 8
Appendix 1: Staff, volunteer and governor Acceptable Use Agreement 9
Appendix 2: Parent/carer digital-use agreement 10
Appendix 3: EYFS and KS1 - child-friendly online safety agreement 11
Appendix 4: KS2 pupil Acceptable Use Agreement 11
Appendix 5: Online safety incident response - quick guide 12
Appendix 6: Related national guidance and resources 12

Approved by	Governing Board
Approval date	September 2026
Policy lead	Executive Headteacher / Heads of School/Setting Leads/Designated Safeguarding Leads
Technical lead	Jartech
Next review due	September 2027 (or sooner following significant change)

1. Purpose and status

Connected Futures Partnership Federation (CFP) recognises that children live and learn in a world in which online and offline experiences are closely connected. Online safety is therefore an integral part of safeguarding, child protection, behaviour, curriculum, data protection and digital leadership.

This policy sets out the federation's expectations for safe, responsible and educationally purposeful use of digital technology. Any online safety concern that may involve harm to a child must be managed through the Child Protection and Safeguarding Policy and the school's safeguarding procedures.

The policy has been rebuilt from the federation's previous LGfL-informed policy and updated for Keeping Children Safe in Education (KCSIE) 2026, current DfE filtering and monitoring standards, current DfE digital technology standards and developments in generative artificial intelligence (AI).

2. Scope

This policy applies to pupils, staff, governors, volunteers, contractors, visitors and other users of school digital systems, and to school-related use of technology whether on or off site. It includes school-owned and personal devices where their use affects safeguarding, professional conduct, the school community or school systems.

It should be read with the CFP Child Protection and Safeguarding Policy, Filtering and Monitoring Policy, Behaviour Policy, Child-on-Child Abuse Policy, Low-Level Concerns Policy, Data Protection Policy, Mobile Phone arrangements, Staff Code of Conduct and relevant Acceptable Use Agreements.

3. The four areas of online risk

CFP uses the established four-area model for understanding online risk:

Area	Examples
Content	Illegal, harmful, age-inappropriate, misleading or extremist material; pornography; self-harm or suicide content; hate; misinformation/disinformation; harmful AI-generated content.
Contact	Grooming, exploitation, coercion, harassment, bullying, scams, radicalisation, unsafe contact with adults or peers, and inappropriate interaction with AI systems or bots.
Conduct	Online bullying, sexual harassment, sharing nude or semi-nude images, abuse, threats, impersonation, privacy breaches, harmful challenges, illegal activity and unsafe digital footprints.
Commerce	Scams, phishing, gambling-like features, inappropriate advertising, financial exploitation, in-app purchases and other commercial risks.

4. Principles

- Children have a right to be protected from harm online as well as offline.
- Filtering and monitoring support safeguarding but do not replace supervision, education, professional curiosity or reporting.
- Online safety education should build knowledge, critical thinking, resilience and confidence to seek help.
- Restrictions should be proportionate and should not unreasonably impede teaching, learning, SEND accessibility or legitimate research.
- Technology changes quickly; policy, risk assessment, staff knowledge and technical controls must therefore be reviewed regularly.
- Children's views and experiences should inform the school's approach.
- AI is treated as part of online safety, safeguarding, data protection, intellectual property and curriculum practice - not as a separate risk universe.

5. Roles and responsibilities

Role	Key responsibilities
Governing Board / safeguarding governor	Ensure appropriate online safety arrangements; hold leaders to account; ensure filtering and monitoring are effective; receive assurance about review, incidents, training and emerging risks.
Executive Headteacher	Provide federation-wide leadership; ensure online safety is integrated with safeguarding; allocate responsibilities; ensure resources, training and review arrangements are in place.
Heads of School	Implement this policy locally; ensure staff understand procedures; ensure concerns are acted upon; maintain links between curriculum, safeguarding and technical arrangements.
Designated Safeguarding Lead (DSL)	Take lead responsibility for online safeguarding; understand local filtering and monitoring arrangements; respond to concerns; identify patterns; liaise with IT, leaders, families and agencies.
SLT digital / online safety lead where designated	Coordinate curriculum and operational online safety work with the DSL; support policy review, training and pupil voice.
IT support / network provider	Maintain secure systems; implement approved filtering and monitoring controls; preserve appropriate logs; report safeguarding concerns promptly; support annual and change-triggered review.
Curriculum / computing leaders	Ensure progressive, age-appropriate online safety and digital literacy education, including AI literacy, misinformation, privacy, copyright and reporting.
All staff and volunteers	Follow the AUA; model safe professional behaviour; supervise appropriately; report concerns immediately; never bypass safeguarding controls without authorisation.
Pupils	Use technology responsibly; follow age-appropriate agreements; protect passwords and personal information; report anything worrying, harmful or unsafe.
Parents/carers	Support safe use, age restrictions and reporting; raise concerns with school; work with school where an online incident affects a child.

6. Safeguarding and reporting concerns

Any member of staff who becomes aware of an online safety concern involving a child must act in accordance with the Child Protection and Safeguarding Policy. The DSL or deputy DSL is the usual first point of contact. Staff must not investigate a safeguarding concern beyond what is necessary to establish the immediate facts and keep the child safe.

- Where a child is in immediate danger, emergency services should be contacted.
- Concerns about an adult working with children must follow the allegations / low-level concerns route as appropriate. A concern about the Executive Headteacher must be referred through the route set out in the safeguarding policy.
- Potentially criminal or illegal content will be handled carefully and referred to the police, Internet Watch Foundation, CEOP or another relevant body where appropriate.
- Staff must not deliberately view, copy, download or forward suspected illegal child sexual abuse material. Preserve the device/context and seek safeguarding advice.
- Online incidents may require coordinated action under safeguarding, behaviour, anti-bullying, child-on-child abuse, Prevent or disciplinary procedures.

7. Nude and semi-nude images and sexual content

Incidents involving the sharing of nude or semi-nude images or videos by children will be managed using current UKCIS guidance and the CFP safeguarding procedures. Staff must not view, copy, print, save or forward an image unless specifically required and authorised by the appropriate safeguarding/law-enforcement process.

The response will consider coercion, exploitation, age, power imbalance, repetition, distribution, threats, blackmail, AI manipulation or 'nudification', and whether the image may constitute child sexual abuse material. The welfare of the child remains central.

8. Filtering and monitoring

CFP maintains a separate Filtering and Monitoring Policy because this is a substantial safeguarding and technical area. This Online Safety Policy should be read alongside it.

- Filtering is preventative: it limits access to harmful and inappropriate content.
- Monitoring is reactive: it helps identify activity that may indicate safeguarding, welfare or security concerns.
- The Governing Board has overall responsibility for ensuring appropriate systems are in place.
- A member of SLT leads the operational approach; the DSL leads the safeguarding response; IT support provides technical expertise.
- Filtering and monitoring are reviewed at least annually and when there is a significant change in technology, risk, provider, configuration or use.
- Reviews consider SEND, EAL, curriculum needs, remote/BYOD access where applicable, generative AI, dynamic content, incidents, technical limitations and over-blocking.
- High-risk monitoring alerts must be escalated promptly; technical monitoring does not replace in-person supervision.

9. Generative artificial intelligence (AI)

Generative AI can support teaching, learning and administration, but its use must be purposeful, age-appropriate, secure and consistent with safeguarding, data protection, copyright and professional standards. The school may approve different tools or use cases for staff and pupils.

- Pupils may only use generative AI in school where the school has approved the tool/use case and appropriate supervision and safeguards are in place.
- Age restrictions and terms of service must be followed.
- Staff and pupils must not enter personal, special-category, confidential or safeguarding information into an AI tool unless the tool and processing have been specifically approved for that purpose.
- Users should assume AI outputs can be inaccurate, biased, fabricated, unsafe or inappropriate and must verify important information.
- AI-generated material must not be used to impersonate, bully, sexualise, exploit or humiliate another person, including through deepfakes or 'nudification'.
- AI use must respect intellectual property and assessment expectations; pupils should be taught when acknowledgement of AI assistance is required.
- Schools will consider DfE generative AI product safety standards when assessing tools intended for educational use.
- Filtering and monitoring risk assessments will consider generative AI, including tools that can access live web content or generate images, audio or video.

10. Online safety education

Each school will provide a planned, progressive online safety curriculum through computing and other relevant curriculum areas. Teaching will be adapted to age, development, SEND, communication needs and the technology pupils are likely to encounter.

- privacy, personal information, passwords and digital footprints;
- healthy relationships, consent, respectful communication and online bullying;
- grooming, exploitation, coercion and how to seek help;

- nude/semi-nude imagery and sexualised content at an age-appropriate level;
- misinformation, disinformation, manipulated media, deepfakes and source evaluation;
- generative AI literacy, including limitations, bias, verification and safe use;
- copyright, ownership, plagiarism and responsible creation;
- scams, phishing, advertising, gambling-like mechanics and commercial pressure;
- extremism, hate and harmful content; and
- how and where to report concerns, including trusted adults and appropriate reporting services.

11. Staff and governor training

Online safety forms part of safeguarding induction and regular safeguarding updates. Training will reflect emerging technology and risks, including filtering and monitoring and generative AI. Governors receive sufficient information and training to discharge their oversight responsibilities.

Staff with specific responsibilities - including DSLs, technical staff and relevant leaders - will maintain role-appropriate knowledge of systems, risks, escalation routes and current guidance.

12. Parents and carers

Schools will provide accessible information to parents/carers about online safety, school expectations and emerging risks. Parents/carers are encouraged to talk regularly with children about online experiences, use age-appropriate controls, understand platform age restrictions and report concerns.

The school recognises that online incidents originating outside school may still affect safeguarding, behaviour, attendance or relationships in school and may require a school response.

13. Accounts, passwords and access

- Users must use individual accounts where provided and must not share passwords.
- Multi-factor authentication will be used for systems where required or appropriate.
- Passwords must be strong and changed promptly if compromise is suspected; arbitrary routine changes will only be required where system/security arrangements justify them.
- Staff must lock devices or log out when unattended and must not permit pupils to use staff accounts.
- Access rights will follow the principle of least privilege and will be removed or amended promptly when roles change or users leave.
- Guest or temporary access will be controlled and limited to what is necessary.

14. Cyber security and technical resilience

Schools will work with their IT support to maintain appropriate cyber security, patching, anti-malware, backups, secure configuration, access control, incident response and disaster recovery arrangements in line with current DfE standards and the school's risk profile.

Users must not install unauthorised software, disable security controls, use tools designed to bypass filtering, or connect unapproved devices or storage media where this would create a security risk. Suspected phishing, malware, credential compromise or data breach must be reported promptly.

15. Email, messaging and communication

- Staff will use school-approved accounts and platforms for professional communication.
- Personal email, personal messaging accounts and personal social-media accounts must not be used to communicate privately with pupils.
- Communication with pupils and families must be professional, necessary, transparent and capable of appropriate oversight.
- Staff should be alert to phishing, impersonation, malicious links and AI-enhanced scams.
- Sensitive information must only be sent using approved secure methods.

16. Online learning and collaboration platforms

School-approved learning platforms will be configured and used in ways appropriate to pupils' age and safeguarding needs. Staff will supervise use, ensure links and resources are suitable, and report misuse or concerning content.

Remote or blended learning must maintain professional boundaries. Staff should use approved accounts and systems, consider what can be seen or heard in the background, and follow safeguarding arrangements for one-to-one or live interaction.

17. Social media and professional boundaries

- Staff must keep personal and professional online relationships appropriately separate.
- Staff must not accept or initiate social-media connections with current pupils through personal accounts.
- Personal online activity must not disclose confidential information, undermine safeguarding, harass others, or compromise the employee's professional role.
- Staff should not post identifiable information about pupils, families or colleagues without an appropriate lawful and professional basis.
- School-approved social-media accounts must have clear ownership, access and moderation arrangements.

18. Mobile phones, wearable and personal devices

Each school will communicate its local arrangements for pupil mobile phones and smart/wearable devices. These arrangements must be consistent with safeguarding, behaviour and DfE expectations and may differ by age and site.

- Staff personal phones must be stored and used in accordance with safeguarding and staff-conduct expectations and must not be used to photograph or record pupils.
- School devices should be used where staff need to contact pupils or families for school purposes.
- Personal devices must not be used to circumvent school filtering, monitoring or network controls.
- Where a device may contain evidence of a safeguarding or criminal concern, staff must not conduct an intrusive search of digital content simply because the device is on school premises. The matter must be referred to a senior leader/DSL and handled under applicable search, safeguarding and legal procedures.

19. Images, video and audio

Images, video and audio of pupils are personal data and will be created, stored and published in accordance with data protection requirements, safeguarding considerations and the school's privacy information. The legal basis for routine educational use is not automatically parental consent in every circumstance; consent will be obtained where consent is the appropriate lawful basis.

- Staff must use school-approved devices and systems for pupil images and recordings.
- Personal devices must not be used to take or store images of pupils.
- Published material will avoid unnecessary identifying information and will consider safeguarding risks before linking names and images.
- Parents/carers attending events will be reminded of expectations about photographing or sharing images of other children.
- AI-generated or manipulated images involving identifiable children or staff are subject to the same safeguarding, conduct and data-protection expectations and may present additional risks.

20. Data protection and privacy

Personal data will be processed in accordance with UK GDPR, the Data Protection Act 2018 and CFP data-protection arrangements. Systems and apps must be assessed before use where they process personal data, and Data Protection Impact Assessments will be completed where required.

Children should be given age-appropriate information about how school technology may filter, log or monitor activity. Monitoring will be proportionate, safeguarding-led and consistent with privacy and data-protection obligations.

21. Digital accessibility and inclusion

Online safety controls should support equitable access. Schools will consider accessibility, SEND, communication needs and assistive technology when selecting or configuring digital tools. A safety control should not be removed simply because it creates a barrier; instead, leaders and technical staff should seek a safe and reasonable solution.

22. Digital images, copyright and intellectual property

Staff and pupils will be taught to respect copyright, licensing, attribution and ownership. AI-generated content can create additional intellectual-property uncertainty; users must follow school guidance and should not assume that generated content is free from copyright or other rights.

23. Incident recording, monitoring and learning

Significant online safety incidents will be recorded through the school's agreed safeguarding/behaviour systems as appropriate. Leaders will identify themes and repeat concerns, including patterns involving platforms, locations, cohorts, vulnerable pupils, AI, sexual content, bullying, filtering breaches or cyber incidents.

Learning from incidents will inform curriculum, staff training, family communication, technical configuration and policy review. Governors will receive appropriate assurance information without compromising individual confidentiality.

24. Review of this policy

This policy will be reviewed at least annually and sooner following significant statutory or technological change, a serious incident, a material change to systems/providers, or evidence that current arrangements are not effective.

Appendix 1: Staff, volunteer and governor Acceptable Use Agreement

The federation may maintain the AUA as a separate operational document for signature; where it does so, the current standalone version should be read as forming part of the implementation of this policy.

I understand that school digital systems are provided to support education, safeguarding and legitimate professional activity. I agree that:

- I will use school technology professionally, lawfully and in accordance with CFP policies.
- I will keep passwords and authentication methods secure and will not use another person's account.
- I will use approved school accounts and communication systems for school business.
- I will protect confidential and personal information and use approved secure storage and transfer methods.
- I will not enter identifiable, confidential, special-category or safeguarding information into generative AI unless the tool and processing have been specifically approved for that purpose.
- I will check AI-generated content for accuracy, bias, safety and appropriateness before relying on or sharing it.
- I will not attempt to bypass filtering, monitoring, security or access controls.
- I will report accidental access to harmful content, safeguarding concerns, filtering/monitoring failures, phishing, malware or suspected data breaches promptly.
- I will not use a personal device to photograph, film or record pupils.
- I will maintain professional boundaries online and will not communicate privately with pupils through personal accounts.
- I will respect copyright, licensing and intellectual-property requirements.
- I understand that use of school systems may be logged and monitored for safeguarding, security and legitimate operational purposes.
- I will return school equipment and cooperate with secure account/device closure when my role ends.
- I understand that serious or deliberate misuse may lead to safeguarding, disciplinary or legal action.

Name: _____ Role: _____

Signature: _____ Date: _____

Appendix 2: Parent/carer digital-use agreement

CFP schools use digital technology to support learning and communication. The school takes proportionate steps to keep children safe, including education, supervision, filtering and monitoring. No technical system can remove every online risk.

- I will support my child to follow the school's age-appropriate digital-use expectations.
- I will encourage my child to tell a trusted adult if something online worries, frightens or upsets them.
- I will contact the school if an online issue is affecting my child's safety, wellbeing, attendance or relationships in school.
- I understand that the school may respond to harmful online behaviour that occurs outside school where it affects pupils or the school community.
- I will respect the privacy of other children and staff when taking or sharing photographs or recordings at school events.
- I will support age restrictions and safe, supervised use of online services and AI tools.
- I understand that school internet and digital activity may be filtered and monitored for safeguarding and security.

Child's name: _____ Class: _____

Parent/carer name: _____

Signature: _____ Date: _____

The following agreements should be adapted and presented in a way that is accessible and meaningful to each child, taking account of their age, stage of development, SEND, communication needs and level of understanding. This may include the use of simplified language, symbols, photographs, visuals, social stories or other appropriate communication supports.

Appendix 3: EYFS and KS1 - child-friendly online safety agreement

A child does not need to be able to read or sign the agreement independently; adults should ensure that the expectations have been explored with them in a way they can understand.

- I ask an adult before I use a new website, app or online tool.
- I keep my name, password and personal information private.
- I am kind when I use technology.
- I only take or share pictures when a trusted adult says it is okay.
- If I see or hear something that worries me, I stop and tell a trusted adult.
- I do not click strange links or messages.
- I know that things made by computers and AI are not always true.
- I use school devices and accounts in the way my teacher shows me.

Child: _____ Class: _____

We have discussed these rules in class. Date: _____

Appendix 4: KS2 pupil Acceptable Use Agreement

- I will use school technology for learning and approved activities.
- I will keep passwords private and will not use another person's account.
- I will be respectful and kind online and will report bullying, threats or harmful content.
- I will not share personal information, images or recordings without permission.
- I will tell a trusted adult if I see something sexual, violent, hateful, frightening or otherwise worrying.
- I will not try to bypass school filtering, monitoring or security.
- I will only use AI tools when my teacher/school says I may, and I will follow age restrictions and instructions.
- I will not put personal or private information into an AI tool.
- I know AI can make things up or get things wrong, so I will check important information.
- I will not use AI or editing tools to create fake, embarrassing, sexual or harmful material about another person.
- I will respect copyright and explain when work is not entirely my own where my teacher requires this.
- I understand that the school may check activity on school systems to help keep people safe.

Pupil: _____ Class: _____

Signature: _____ Date: _____

Appendix 5: Online safety incident response - quick guide

Step	Action
1. Make safe	Address immediate danger; stop harmful contact/activity where this can be done safely; do not unnecessarily view or copy harmful material.
2. Report	Tell the DSL/deputy DSL immediately where a child may be at risk. Follow the adult-concern route if the concern involves staff.
3. Preserve	Preserve relevant device/context, URLs, usernames, times and factual information without forwarding illegal or sexual imagery.
4. Assess	DSL considers safeguarding, criminality, child-on-child abuse, sexual imagery, exploitation, Prevent, bullying, SEND and vulnerability.
5. Refer	Contact police, children's social care, LADO, CEOP, IWF or other agencies where thresholds/needs indicate.
6. Support	Support the child affected; communicate with parents/carers where appropriate and safe; consider safety planning.
7. Record	Record concern, decisions, rationale, actions and outcome on the appropriate school system.
8. Learn	Review whether curriculum, supervision, filtering/monitoring, staff training or technical controls need to change.

Appendix 6: Related national guidance and resources

- Keeping Children Safe in Education 2026 (DfE).
- Meeting digital and technology standards in schools and colleges, including Filtering and Monitoring and Cyber Security core standards (DfE).
- Generative artificial intelligence (AI) in education and Generative AI: product safety standards (DfE).
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS).
- Education for a Connected World (UKCIS).
- UK Safer Internet Centre and Professionals Online Safety Helpline.
- CEOP / National Crime Agency reporting and education resources.
- Internet Watch Foundation reporting arrangements.
- Information Commissioner's Office guidance for schools and children's data.