

Online Safety Policy

Policy owner	Executive Headteacher
Designated Safeguarding Lead	Rachel Vaughan
Online Safety Lead – Whittington	Sam Druce
Online Safety Lead – Morda	Andrew Lyons
Safeguarding Governor	Jade Wright
Applies to	Both schools, including the Whittington nursery
Approved by	Governing Body – Autumn 2026
Review date	Autumn 2027, or earlier following significant change or incident

1. Purpose and commitment

Pathway Primary Federation recognises that technology is integral to learning, communication and participation in modern life. We will enable pupils and staff to use it confidently, creatively and responsibly while protecting them from online harm. Online safety is a safeguarding responsibility and is embedded in our culture, curriculum, systems and professional practice.

Our approach reflects our Christian vision and values. The same standards of respect, honesty and care apply online as offline.

2. Scope

This policy applies to governors, employees, agency and supply staff, volunteers, contractors, visitors, pupils and families using school systems, networks, accounts, services or devices. It also applies to personal technology used on school premises or where online behaviour outside school affects a pupil, staff member, the safe operation of either school or the reputation of the Federation.

It should be read with the Safeguarding and Child Protection, Behaviour, Anti-Bullying, Data Protection, Prevent, RSHE, Staff Code of Conduct, Mobile Phone, Photography, Remote Learning and Acceptable Use arrangements.

3. Statutory and guidance framework

- Keeping Children Safe in Education 2026;
- DfE Filtering and Monitoring: Core Standard, updated August 2026;
- DfE Teaching Online Safety in Schools guidance;
- Education and Inspections Act 2006 and Education Act 2011;
- UK GDPR and Data Protection Act 2018;
- Counter-Terrorism and Security Act 2015 and Prevent duty guidance 2023;
- Voyeurism (Offences) Act 2019, Online Safety Act 2023 and relevant communications, harassment, sexual-offences, copyright and computer-misuse legislation; and
- current UKCIS guidance, including responding to incidents involving nude or semi-nude images.

4. Understanding online risk: the four Cs

Area	Examples
Content	Being exposed to illegal, inappropriate or harmful material, including pornography, violence, suicide and self-harm content, racism, misogyny, misinformation, extremist material and AI-generated or manipulated content.
Contact	Harmful interaction with other users, including grooming, coercion, exploitation, harassment, unwanted contact, scams or contact with adults posing as children.
Conduct	Personal online behaviour that increases harm, including cyberbullying, abusive messages, sharing private information or images, sexualised behaviour, creating or forwarding harmful content, and unsafe use of artificial intelligence.
Commerce	Risks such as gambling-style features, inappropriate advertising, phishing, financial scams, in-app purchases and exploitation of personal data.

Risk may occur through websites, search, social media, messaging, livestreaming, gaming, wearable technology, connected toys, virtual or augmented reality, generative AI, cloud services and any emerging technology.

5. Roles and responsibilities

Who	Responsibilities
Governing Body	Holds overall strategic responsibility; ensures appropriate filtering and monitoring; approves the policy; appoints a responsible governor; receives assurance and ensures an annual review.
Executive Headteacher	Provides executive oversight, resources and accountability; approves exceptional access and ensures consistent arrangements across both schools.

Who	Responsibilities
DSL	Leads safeguarding and online safety; reviews relevant monitoring reports; responds to concerns; ensures records and referrals; provides assurance to governors.
Online Safety Leads	Coordinate curriculum and awareness at each school; support staff; review trends and policy implementation with the DSL and senior leaders.
Heads of School	Ensure day-to-day implementation, staff supervision, incident escalation and communication with families on each site.
IT support provider	Maintains technical controls, security, filtering and monitoring; supplies intelligible reports; implements authorised changes; reports safeguarding concerns promptly.
All staff and volunteers	Model professional use, provide active supervision, follow acceptable-use rules, preserve evidence appropriately and report concerns immediately.
Pupils	Use technology responsibly, follow age-appropriate agreements, protect passwords and report anything worrying or unsafe.
Parents and carers	Support safe use at home, follow school arrangements, report concerns and respect children's privacy when sharing images or information.

6. Education and prevention

Online safety is taught progressively through computing, RSHE, wider curriculum work, assemblies and responsive teaching. Pupils will learn to:

- recognise the four Cs and assess risk rather than rely only on technical controls;
- protect personal information, accounts, passwords and digital reputation;
- understand consent, privacy, respectful communication and the permanence and reach of online sharing;
- recognise grooming, coercion, scams, manipulation, misinformation and harmful algorithms;
- use search, social media and generative AI critically, checking accuracy, bias, provenance and age restrictions;
- understand copyright, ownership, plagiarism and when AI-assisted work must be acknowledged;
- block, mute and report users or content appropriately, retain relevant evidence and seek help from a trusted adult; and
- understand that reporting accidental access or a mistake promptly is the safest response and will not, by itself, lead to punishment.

Teaching will be age-appropriate, inclusive and adapted for pupils with SEND, communication needs, EAL or additional vulnerability. Staff will avoid creating fear or blame and will revisit key messages regularly.

7. Filtering and monitoring

The Federation will maintain filtering and monitoring appropriate to the age and risk profile of pupils, the technology in use and the needs of each site. Filtering is preventative; monitoring identifies concerning activity so that staff can respond. Neither replaces effective classroom supervision.

- A senior leader, the DSL, the safeguarding governor and IT support will have clearly documented responsibilities.
- Provision will be reviewed at least annually and following a serious incident, material system change, new device or service, or change in working practice.
- The review will consider all school-managed devices on and off site, staff and pupil profiles, guest access, apps, generative-AI products, SEND/EAL needs, local risks, alerts, incidents and technical limitations.
- Filtering will use current illegal-content blocklists, including IWF and CTIRU arrangements, and will block harmful content without unreasonably restricting teaching and learning.
- Temporary filtering exceptions require documented senior-leader approval, a stated purpose and duration, and subsequent removal.
- Monitoring will combine active staff supervision with technical or network monitoring appropriate to risk. High-risk alerts will be escalated immediately; routine reports will be reviewed at least weekly.
- Checks, results, decisions and actions will be logged. New devices and services will be tested before deployment.
- Users will be told that school networks and devices are filtered and monitored. Any monitoring provider will be subject to due diligence, a DPIA where required and appropriate privacy information.

8. School systems, accounts and cyber security

- Users must have individual accounts wherever practicable and must not share passwords or authentication codes.
- Passwords must be strong and unique; multi-factor authentication will be used where available and proportionate.
- Devices must be locked when unattended and updated promptly. Security controls must not be disabled or bypassed.
- School information must be stored and transferred only through approved systems. Personal email or consumer messaging must not be used for confidential school information.
- Only authorised encrypted removable media may be used. Lost devices, suspected phishing, malware, data breaches or compromised accounts must be reported immediately.
- Software, apps, browser extensions, cloud services and AI tools require school approval before use with pupils or school information.
- Access will be removed or amended promptly when roles change or people leave. Privileged access will be restricted and reviewed.

9. Artificial intelligence

Generative AI can support learning and staff workload but may produce inaccurate, biased, unsafe or fabricated material and may collect information entered into it. The following rules apply:

- Pupils may use only school-approved AI tools, for an authorised learning purpose and with appropriate adult oversight.
- Personal, special-category, safeguarding, confidential or identifiable pupil information must not be entered into public AI tools.
- Staff must verify outputs, remain professionally accountable and consider copyright, bias, hallucination, age restrictions and safeguarding implications.
- AI must not be used to impersonate, deceive, bully, generate sexual or violent content, defeat assessment, or make automated decisions about pupils or staff.
- AI-generated or AI-assisted work must be acknowledged where directed. Teachers will make expectations clear for each task.
- New AI products require safeguarding, data-protection and technical assessment, including DPIA consideration, before adoption.

10. Personal devices, mobile phones and wearable technology

Pupil use of personal mobile phones and comparable communication technology during the school day is prohibited, except where an individually agreed exemption or reasonable adjustment applies. Devices brought to school must follow each school's collection, storage and retrieval arrangements. Smart watches or other connected devices must not be used to communicate, record or access online services during the school day.

Staff personal devices must be silenced and stored securely while supervising pupils, except for an authorised work or emergency purpose. Staff must not use personal devices to photograph or record pupils, store school information or communicate privately with pupils. Visitors and families must follow instructions regarding photography and recording at events.

11. Images, video, livestreaming and intimate imagery

- School images and recordings will be captured on approved devices, stored securely and used in accordance with privacy information and consent arrangements.
- Names and images will not be combined in a way that creates unnecessary risk. Livestreaming requires specific approval and appropriate access controls.
- Upskirting, voyeurism, sexual harassment and creating or sharing sexual images without consent are prohibited and may constitute criminal and safeguarding matters.
- Any incident involving nude or semi-nude imagery of a child must be reported immediately to the DSL. Staff must not view, copy, print, forward or ask a child to display imagery unless the DSL determines that viewing is necessary and lawful under current guidance.
- Devices must not be searched beyond authorised powers and procedures. Police advice will be sought where an offence or serious risk may be involved.

12. Communication, social media and professional boundaries

- Communication with pupils and families must use approved school accounts, platforms and channels.

- Staff must not accept pupils as contacts on personal social-media accounts or use private messaging to communicate with them.
- Staff must maintain confidentiality, professional boundaries and appropriate language online and must not post content that compromises safeguarding, public confidence or the Federation's reputation.
- School social-media accounts require authorisation, more than one appropriate administrator where practicable, secure credentials and active moderation.
- Concerns about online harassment or abuse of staff will be addressed under safeguarding, behaviour, complaints, staff-wellbeing and legal procedures as appropriate.

13. Cyberbullying and harmful behaviour outside school

Cyberbullying will be addressed under the Anti-Bullying and Behaviour policies and, where appropriate, the Safeguarding and Child Protection Policy. The school may respond to online behaviour outside school when it affects another pupil or staff member, threatens safety, disrupts learning or the orderly running of the school, or damages the school's reputation. Responses will be proportionate and will consider age, SEND, context, intent, impact and recurrence.

14. Reporting and responding to incidents

If a child is in immediate danger, call 999. Any safeguarding concern must be reported to Rachel Vaughan, DSL, or a deputy DSL without delay and recorded on CPOMS.

1. Make the situation safe. Listen calmly, reassure the child and avoid blame or promises of confidentiality.
2. Do not investigate beyond what is necessary to establish immediate facts. Do not unnecessarily view, download, forward or delete potentially illegal or harmful content.
3. Preserve available evidence safely, including URLs, usernames, dates and screenshots where lawful and appropriate.
4. Report and record the incident through the correct route: DSL/CPOMS for safeguarding; senior leader for behaviour or staff conduct; IT support for technical containment; DPO for a possible personal-data breach.
5. The DSL or senior leader will assess content, contact, conduct and commerce risks; consider Prevent, child-on-child abuse, sexual violence or harassment, exploitation, self-harm, criminality and data protection; and decide referrals or advice required.
6. Inform parents or carers unless this would increase risk, compromise an investigation or conflict with safeguarding advice.
7. Provide support, proportionate consequences and follow-up; review whether controls, teaching, risk assessment or policy need to change.

15. Incident routing

Concern	Immediate route
Child protection, grooming, sexual harm, self-harm, exploitation, serious threats	DSL immediately; CPOMS; emergency services or external safeguarding referral as required

Concern	Immediate route
Terrorism or radicalisation concern	DSL/Prevent lead immediately; follow Notice, Check, Share and current referral route
Nude or semi-nude imagery involving a child	DSL immediately; follow current UKCIS guidance; do not copy or forward
Cyberbullying or pupil misuse	DSL if safeguarding is involved; otherwise Head of School/teacher under Behaviour and Anti-Bullying policies
Staff conduct, allegation or low-level concern	Executive Headteacher or Chair where appropriate; follow safeguarding staff-concern procedures
Personal-data breach	Executive Headteacher/Operations Manager and Classroom365 as DPO; follow Data Protection Policy
Malware, compromised account or network incident	IT support and senior leader immediately; preserve evidence and contain risk
Illegal content or suspected crime	DSL/Executive Headteacher; obtain police or specialist advice; call 999 if immediate danger

16. Acceptable use and breaches

Access to school technology is conditional on following the relevant acceptable-use agreement. Agreements will be explained in age-appropriate language and revisited regularly. A breach will be assessed according to risk and context. Responses may include education and support, parental involvement, restricted access, recovery of school equipment, consequences under the Behaviour Policy, disciplinary action, safeguarding referral or police involvement. Safeguarding and welfare take precedence over punishment.

17. Training, communication and partnership

- Online safety forms part of safeguarding induction and regular staff updates. Staff with designated roles receive training appropriate to their responsibilities.
- Governors receive sufficient information and training to provide challenge and assurance, particularly for filtering and monitoring.
- Pupils and families receive regular, practical information about current risks, reporting routes, age restrictions, privacy, gaming, social media, scams and emerging technology.
- The Federation will work with IT providers, the local authority, police, social care, health services and specialist organisations where appropriate.

18. Equality, SEND and inclusion

Online harms can disproportionately affect pupils with SEND, communication needs, experience of care, mental-health needs or other vulnerabilities. Risk assessment, teaching, reporting and support will be adapted accordingly. Reasonable adjustments

will be made without reducing safeguarding expectations. Staff will challenge misogyny, racism, homophobia, biphobia, transphobia, ableism, religious hatred and other prejudice online and offline.

19. Data protection and monitoring privacy

The Federation will process monitoring, account and incident information only where lawful and necessary. Privacy notices will explain relevant monitoring. Access to reports and records will be restricted, retention will be proportionate and suppliers will be subject to contractual and security controls. Classroom365 is the Federation's Data Protection Officer. Data protection does not prevent necessary safeguarding information sharing.

20. Monitoring and review

The DSL, online-safety leads, senior leaders and IT support will review incidents, alerts, pupil voice, curriculum coverage, staff training and technical controls. Filtering and monitoring provision will be formally reviewed at least annually with governor involvement, and checks will be recorded. Governors will receive anonymised assurance information. This policy will be reviewed annually and sooner following new guidance, a significant incident or material technological change.

Appendix A — Staff, governor and volunteer acceptable use

I understand that access to Federation systems and information is provided for authorised professional purposes and that safeguarding, confidentiality and professional standards apply at all times. I will:

- use approved accounts, devices, applications and communication channels;
- keep credentials secure, use strong unique passwords and multi-factor authentication where provided;
- lock devices when unattended and report loss, compromise, phishing, malware or a data breach immediately;
- store and transfer school information only through approved systems and follow the Data Protection Policy;
- maintain professional boundaries and never communicate privately with pupils through personal accounts or devices;
- use only approved devices to photograph or record pupils and follow consent and publication arrangements;
- provide active supervision when pupils use technology and report safeguarding concerns immediately to the DSL;
- not bypass filtering, monitoring or security controls, install unapproved software, or allow unauthorised access;
- use generative AI only as authorised, verify outputs and never enter confidential or identifiable pupil information into public tools;
- respect copyright, licensing, confidentiality and the reputation of pupils, colleagues and the Federation; and
- understand that authorised monitoring and audit may take place and that serious misuse may result in disciplinary, safeguarding or legal action.

Name	
Role	
Signature	
Date	

Appendix B — Pupil acceptable use: Reception and Key Stage 1

Our online-safety promises

- I use school devices only when an adult says I may.
- I ask before I click, download, take a photograph or share something.
- I keep my password private, except when a trusted adult needs to help me.
- I am kind and respectful when I use technology.
- I do not share my name, address, school, photograph or other personal information without an adult's permission.
- If I see or hear something that worries, frightens or confuses me, I stop and tell a trusted adult straight away.
- I know I will not be in trouble simply for telling an adult about something that happened by accident.
- I do not try to get around the school's safety settings.

Pupil name	
Class	
Pupil signature or mark	
Date	

Appendix C — Pupil acceptable use: Key Stage 2

- I use school technology and accounts only for authorised activities and follow adult instructions.
- I keep passwords and personal information private and tell an adult if I think an account is unsafe.
- I communicate respectfully and do not bully, threaten, impersonate or deliberately embarrass anyone.
- I ask permission before taking or sharing images, recordings or someone else's work.
- I check information carefully and understand that websites, social media and AI can be wrong, biased or misleading.
- I use only approved AI tools, follow the teacher's instructions and acknowledge help from AI where required.
- I do not search for, create, save or share illegal, sexual, violent, hateful or otherwise harmful material.
- If harmful content appears, I stop, do not forward or delete evidence, and tell a trusted adult immediately.
- I do not bypass filters, monitoring or security, use another person's account or install unapproved software.
- I understand that school systems and devices are monitored and that the school may respond to harmful online behaviour outside school.

Pupil name	
Class	

Pupil signature	
Date	

Appendix D — Parent and carer partnership statement

Parents and carers are asked to support the Federation by:

- discussing the age-appropriate pupil agreement and reinforcing safe, kind and responsible use at home;
- using parental controls and age settings, while recognising that conversation and supervision remain essential;
- reporting concerns promptly and preserving relevant evidence without circulating harmful content;
- following school rules for mobile phones, photography and recording at events;
- not posting identifiable information, images or complaints about other children online; and

contacting the school if family circumstances or addition



Jan Paul
Interim Chair of Governo



Carl Rogers
Executive Headteacher