



Perseverance Respect Honesty Friendship

Online Safety Policy

Date written	Authorised by	Review Date
January 2026	Governors	January 2027



Contents

1. Aims	4
Content – Exposure to harmful or inappropriate material	4
2. Legislation and Guidance.....	5
3. Roles and Responsibilities	5
3.1 The Governing Board	5
3.2 The Headteacher	6
3.3 The Designated Safeguarding Lead (DSL).....	6
3.4 The ICT Manager / IT Support.....	6
3.5 All Staff and Volunteers.....	6
3.6 Parents/Carers	6
3.7 Visitors and Community Users	7
4. Educating Pupils	7
5. Educating Parents	7
6. Cyber-Bullying	8
7. Acceptable Use	9
8. Mobile Devices	10
9. Staff Devices	10
10. AI and Emerging Tech	11
11. Prevent Duty	12
11.1 Governance, Roles and Oversight.....	12
11.2 Risk Assessment (including online)	12
11.3 Curriculum and Education	12
11.4 Filtering, Monitoring and Alerts	13
11.5 Staff Responsibilities and Training.....	13
11.6 Recognising Concerns (Online Indicators)	13
11.8 Records, Reviews and Governor Reporting	13
11.9 Engagement with Parents/Carers	14
11.10 Links to Related Policies	14

I2. Responding to Misuse	14
I3. Training	15
I4. Filtering & Monitoring	15
I5. Monitoring Arrangements	16
I6. Links with Other Policies	16
Appendix 1 – All Parents / Pupils.....	17
Appendix 2 – Staff, governors, volunteers and visitors - ICT Acceptable Use	19
Appendix 3 – Online Safety Incident and Monitoring Log - Template.....	22
Appendix 4 – Filtering & Monitoring Annual Review Template.....	23
Appendix 5 – Secure AI Providers.....	27
Appendix 6 – Prevent Risk Assessment	28

I. Aims

- Maintain robust processes to ensure online safety for pupils, staff, volunteers, visitors and governors, including mobile and smart technology.
- Identify and support groups of pupils potentially at greater risk online (e.g., SEND, vulnerable learners).
- Deliver a whole-school approach embedded across curriculum, policy, filtering/monitoring and staff development.
- Establish clear mechanisms to identify, intervene and escalate incidents, including filtering/monitoring failures and off-site harms.

The four key categories of risk

Category	Example	Emerging Risk
Content – Exposure to harmful or inappropriate material	• Pornography or sexually explicit material. • Violent or graphic imagery. • Hate speech, racism, misogyny, antisemitism. • Extremist or radicalising material.	• Misinformation and disinformation (e.g., conspiracy theories, fake news). • Harmful online challenges and hoaxes. • AI-generated deepfake images or videos used to mislead or harass.
Contact – Harmful interaction with others online	• Grooming by adults posing as children on social media or gaming platforms. • Pressure from peers to share personal information or explicit images. • Fraudulent contact for financial scams.	• Contact through encrypted messaging apps (e.g., WhatsApp, Telegram). • Recruitment into extremist groups via online forums. • Approaches via live-streaming platforms or influencer communities. • Risks from communication with individuals or groups who may pose a threat.
Conduct – Pupils' own online behaviour	• Cyber-bullying (sending abusive messages, sharing harmful memes). • Sharing nudes or semi-nudes (consensual or non-consensual). • Posting offensive or discriminatory comments.	• Creating or sharing AI-generated explicit content. • Participating in harmful viral trends. • Oversharing personal data on social media.

Commerce – Financial and consumer risks	• Online gambling or gaming with in-app purchases. • Phishing emails and fake websites. • Identity theft and fraud.	• Cryptocurrency scams targeting young people. • Influencer-driven advertising of unsafe products. • Loot boxes and micro transactions in games.
---	---	--

2. Legislation and Guidance

This policy is based on, and should be read alongside:

- **Keeping Children Safe in Education (KCSIE) 2025** (statutory).
- **DfE Filtering and Monitoring Standards** (part of Digital and Technology Standards).
- **Teaching online safety in schools** (DfE, non-statutory).
- **Education for a Connected World** (UKCIS framework for progression).
- **Sharing nudes and semi-nudes: UKCIS guidance (2024 update)**.
- **Searching, screening and confiscation (DfE)** for handling devices.
- **Mobile phones in schools (DfE, Feb 2024)**.
- **Prevent Duty Guidance (Home Office, 2023; in force from 31 Dec 2023)** and **Channel Duty Guidance (2023)**.
- **Cyber Security Standards for schools and colleges (DfE)**.
- **DfE policy on Generative AI in education (2025)** and product safety expectations for AI tools.

This policy also reflects relevant legislation (Education Acts 1996/2006/2011; Equality Act 2010; UK GDPR/Data Protection Act 2018).

3. Roles and Responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. It will ensure:

- Appropriate filtering and monitoring systems are in place on school devices and networks; reviewed at least annually; and block harmful/illegal content without unreasonable impact on teaching and learning.
- Online safety is a running, interrelated theme across safeguarding and related policies.
- Roles for filtering/monitoring oversight are assigned (e.g., DSL lead, IT manager) and their effectiveness is reviewed.
- Regular online safety updates (at least annually) are provided to all staff and governors, including changes to DfE/UKCIS guidance.
- Children are taught how to keep themselves and others safe online through a progressive curriculum.

3.2 The Headteacher

Responsible for ensuring staff understand and consistently implement this policy, and for resourcing filtering/monitoring and staff training.

3.3 The Designated Safeguarding Lead (DSL)

The DSL (and Deputy) take lead responsibility for online safety, including:

- Oversight of filtering/monitoring systems and processes; liaison with IT; and acting on alerts and reports of failures.
- Managing incidents in line with safeguarding procedures; keeping online safety logs; and reporting to SLT/governors.
- Annual online safety risk assessment that reflects evolving risks (including AI, disinformation, encrypted apps).
- Staff training and updates (see Section 11) and promoting use of UKCIS/DFE materials.

3.4 The ICT Manager / IT Support

Responsible for:

- Implementing age-appropriate filtering and effective monitoring on school devices and networks; reviewing at least annually.
- Securing systems against malware; maintaining patches; logging incidents; and supporting investigations.
- Advising on bypass requests for educational purposes, with clear recording and DSL oversight.

3.5 All Staff and Volunteers

All staff and volunteers must:

- Read and follow this policy and the acceptable use agreement; ensure pupils follow theirs.
- Report filtering/monitoring failures, online harms, and device incidents immediately to the DSL.
- Respond appropriately to all reports of online sexual harassment/violence and maintain the attitude “it could happen here.”

3.6 Parents/Carers

The school will share this policy and provide regular information/resources (website, newsletters/workshops/wakeupwednesday). Parents are expected to support acceptable use agreements and raise concerns with school leaders.

School encourages all parents to take a proactive approach to keeping their children safe online. School provide regular materials that will support parents having conversations with their child at home and that regular checking and monitoring of online activity is an established part of home life.

3.7 Visitors and Community Users

Visitors using school systems will be made aware of this policy and asked to sign the relevant acceptable use agreement if applicable.

4. Educating Pupils

Online safety is taught through Computing, PSHE/RSE, and across subjects, mapped to Education for a Connected World to ensure progression from EYFS to KS2 (and beyond where relevant). Coverage includes self-image, online relationships, online bullying, privacy/security, managing online information (including spotting misinformation/disinformation), online reputation, health/wellbeing/lifestyle, and copyright/ownership.

We use ProjectEVOLVE, developed by the UK Council for Internet Safety (UKCIS), to deliver a structured and progressive online safety curriculum. ProjectEVOLVE is based on the Education for a Connected World framework, which identifies key strands of knowledge and skills children need to navigate the digital world safely and responsibly.

What ProjectEVOLVE provides:

- **Strand-based approach:** Covers eight strands including Self-Image & Identity, Online Relationships, Online Bullying, Managing Online Information, Health & Wellbeing, Privacy & Security, Copyright & Ownership, and Online Reputation.
- **Age-appropriate resources:** Each strand is broken down into progressive statements from EYFS through to KS4, ensuring pupils build understanding step by step.
- **Dynamic teaching materials:** Includes discussion prompts, activities, and assessment tools to help teachers tailor lessons to pupils' needs.
- **Focus on critical thinking:** Encourages pupils to question online content, understand risks like misinformation and disinformation, and develop resilience.
- **Integration with safeguarding:** Supports statutory requirements under KCSIE and complements PSHE/RSE and Computing curriculum.

By using ProjectEVOLVE, we ensure pupils receive consistent, evidence-based education on online safety, aligned with national guidance and adapted for SEND and vulnerable learners.

By the end of primary, pupils will know how to recognise risks, harmful content; report concerns; and apply respectful online behaviour, including critical thinking about sources and AI-generated content. By the end of primary, pupils will know how to recognise risks, harmful content and contact; report concerns; and apply respectful online behaviour, including critical thinking about sources and AI generated- content.

Teaching is adapted for SEND and vulnerable pupils to ensure accessibility and appropriate support.

5. Educating Parents

We recognise that parents and carers play a vital role in supporting children to stay safe online. Our approach includes:

- **Regular communication:**
 - We share weekly online safety messages through our school app as part of our *Wake Up Wednesday* initiative, using resources from The National College. These updates

provide practical advice and highlight current risks, trends, and emerging technologies (e.g., social media challenges, scams, AI misuse).

- Messages are concise, accessible, and designed to help families reinforce safe online behaviours at home.
- **Annual Online Safety Workshops:**
 - We run face-to-face or virtual workshops for parents/carers every year. These sessions cover key topics such as managing screen time, privacy settings, preventing online bullying, and understanding new risks like misinformation and AI-generated content.
 - Workshops include practical demonstrations and Q&A opportunities to empower parents with strategies for supporting their children.
- **Policy and resources:**
 - This Online Safety Policy is shared with parents/carers and is available on our website.
 - We signpost families to trusted resources such as UK Safer Internet Centre, Childnet, and National College for further guidance.
- **Proactive engagement:**
 - Parents/carers are encouraged to raise any concerns or queries with the head teacher or DSL.
 - We provide updates during parents' evenings and through newsletters to ensure families remain informed about our online safety approach.

By combining weekly updates, annual workshops, and ongoing communication, we aim to create a strong partnership with parents/carers to keep children safe online.

6. Cyber-Bullying

6.1 Definition

Cyber-bullying is the repetitive, intentional harming of an individual or group through digital platforms, where there is an imbalance of power. It can occur via social media, messaging apps, gaming platforms, email, or any online environment.

Forms of cyber-bullying include:

- Sending abusive or threatening messages.
- Sharing embarrassing images or videos without consent.
- Excluding someone from online groups or chats.
- Impersonating someone online to damage their reputation.
- Posting harmful or discriminatory comments publicly.

Emerging risks:

- Use of AI-generated content (e.g., deepfake images or videos) to humiliate or harass.
- Viral challenges or hoaxes that encourage harmful behaviour.
- Coordinated harassment through anonymous apps or encrypted platforms.

6.2 Prevention

We take a proactive approach to prevent cyber-bullying by:

- Teaching pupils what cyber-bullying is, why it happens, and its impact, through PSHE, RSE, and Computing lessons.
- Embedding discussions about respect, empathy, and responsible online behaviour across the curriculum.
- Using ProjectEVOLVE strands (Online Bullying, Online Relationships) to build resilience and critical thinking.
- Encouraging pupils to report concerns promptly, whether they are victims or bystanders.
- Providing parents/carers with weekly updates (*Wake Up Wednesday*) and annual workshops to help them spot signs and support children.

6.3 Response

When an incident occurs, the school will:

- Act swiftly in line with the Behaviour Policy and Safeguarding Policy.
- Contain harmful material by working with platforms or external agencies where necessary.
- Log all incidents on our safeguarding system and inform parents/carers.
- Apply proportionate sanctions and provide support for both victims and perpetrators.
- Refer to the police if the material is illegal or poses a significant risk.

6.4 Examining Electronic Devices

- Searches and confiscations follow DfE guidance on Searching, Screening and Confiscation.
- Staff must never view indecent images of children; devices suspected of containing such material are handed to the DSL immediately.
- The DSL will follow UKCIS guidance on sharing nudes and semi-nudes, ensuring safeguarding and legal compliance.

7. Acceptable Use

To ensure the safe and responsible use of technology, all users of the school's ICT systems, including pupils, parents/carers, staff, governors, volunteers, and visitors must agree to and sign an **Acceptable Use Policy (AUP)**. These agreements set clear expectations for behaviour and outline consequences for misuse.

Key principles of acceptable use:

- **Educational Purpose Only**
All use of school ICT systems and internet must be for learning, teaching, or fulfilling professional duties. Personal use is not permitted during school hours or on school devices.
- **Respect and Responsibility**
Users must treat others with respect online, avoiding any language or behaviour that is harmful, discriminatory, or offensive. Cyber-bullying, harassment, or intimidation will not be tolerated.
- **Security and Privacy**
 - Keep usernames and passwords secure; never share login details.
 - Do not attempt to bypass filtering or monitoring systems.
 - Protect personal and sensitive information, both your own and others'.
- **Content Restrictions**
 - Do not access, create, or share illegal, harmful, or inappropriate material (including extremist content, pornography, or violent imagery).
 - Do not upload or distribute copyrighted material without permission.
- **Emerging Risks**
 - Do not use AI tools to create harmful, misleading, or plagiarised content.
 - Do not engage in online gambling, scams, or financial transactions using school systems.
- **Monitoring and Compliance**
The school actively monitors internet use through filtering and monitoring systems. Breaches of the AUP may result in sanctions, including loss of access, disciplinary action, or referral to external agencies where appropriate.

8. Mobile Devices

Pupils in Year 5 and 6 may bring certain devices into school but must hand them in to school staff who will store them securely before returning them at the end of the school day. This includes the following items:

- Mobile Phones
- Smartphones
- Smart watches

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff Devices

Staff members are responsible for keeping school devices secure and using them in line with the Acceptable Use Policy (AUP) and Data Protection Policy. This includes:

Device Security

- **Password Protection:** Devices must be secured with strong passwords and, where possible, multi-factor authentication (MFA) for key services such as email and cloud storage.
- **Encryption:** Ensure hard drives are encrypted so data cannot be accessed if the device is lost or stolen.
- **Automatic Lock:** Devices should lock after a short period of inactivity.
- **Regular Updates:** Install all operating system and software updates promptly to maintain security.
- **Anti-virus and Anti-malware:** Keep security software active and updated.

Email and Account Security

- Use **two-factor authentication (2FA)** for email accounts and any system that supports it.
- Never share login credentials or allow others to use your work device.

Acceptable Use and Data Protection

- Work devices must only be used for professional purposes.
- Do not store personal data unrelated to school business.
- Handle pupil and staff data in compliance with GDPR and school privacy notices.
- Avoid saving sensitive data locally; use secure cloud storage provided by the school.

Reporting Concerns

- If a device is lost, stolen, or compromised, or if you suspect a security breach, report immediately to the ICT Manager and DSL.
- Do not attempt to fix security issues yourself and always follow school procedures for escalation.

10. AI and Emerging Tech

Artificial Intelligence (AI) tools and emerging technologies offer opportunities for learning and efficiency but also present new safeguarding and ethical challenges. Our approach ensures safe, responsible, and age-appropriate use, fully aligned with our Safeguarding Policy (Section 12) and statutory guidance.

10.1 Governance and Principles

- AI use in school is governed by the DSL, with technical controls managed by the ICT Manager and strategic oversight by SLT.
- All AI activity complies with:
 - DfE Generative AI: Product Safety Expectations (2025)
 - Filtering and Monitoring Standards for Schools
 - Cyber Security Standards for Schools and Colleges
- AI use is reviewed alongside filtering/monitoring and safeguarding risk assessments.

10.2 Staff Use

- Staff may use AI for specific professional tasks, including:
 - Generating or adapting teaching materials.
 - Drafting letters and emails.
 - Checking spelling and grammar of anonymised report comments.
 - Supporting administrative tasks (e.g., risk assessments, care plans).
- **Rules for staff use:**
 - Do not input personal or sensitive data into AI tools.
 - Check outputs for accuracy, bias, and appropriateness before use with pupils.
 - Comply with GDPR, Acceptable Use Policy, and Staff Code of Conduct.

10.3 Pupil Use and Curriculum

- AI use by pupils is permitted only under teacher supervision in a controlled classroom environment.
- Activities must be age-appropriate, linked to learning objectives, and supported by a risk assessment.
- AI literacy is taught through ProjectEVOLVE, mapped to Education for a Connected World, covering:
 - Risks of misinformation/disinformation and conspiracy theories.
 - Deepfakes and synthetic media.
 - Algorithmic bias and ethical considerations. (Cross-reference: Safeguarding Policy Section 3.6 – Curriculum and Online Safety)

10.4 Risks and Safeguards

- **Emerging risks:**
 - AI-generated harmful or misleading content.
 - Deepfake images/videos used for bullying or harassment.
 - Synthetic extremist material linked to radicalisation.
- **Safeguards:**
 - AI access is disabled by default and enabled only by teachers for defined tasks.
 - All AI activity is subject to filtering and monitoring; any failure or concerning alert is logged and escalated to the DSL and ICT Manager.
 - Suppliers of AI tools are assessed against DfE product safety expectations before adoption.

10.5 Reporting and Records

- Any AI-related concern (unsafe output, data entry breach, deepfake bullying, Prevent risk) must be reported immediately to the DSL and recorded on CPOMs as an online safety incident.
- AI incidents are included in termly governor reports and annual safeguarding reviews.

10.6 Training

- AI training is included in annual staff online safety and cybersecurity updates.
- Governors receive updates on AI risks and usage as part of safeguarding oversight.

11. Prevent Duty

Safeguarding against radicalisation and extremism is part of our whole-school approach to safeguarding. Our procedures are fully aligned with our Safeguarding Policy (see Section 12: Safer use of the internet and digital technology and Radicalisation & Extremism), and comply with the Prevent Duty Guidance (Home Office, 2023; in force from 31 Dec 2023) and Channel Duty Guidance (2023).

11.1 Governance, Roles and Oversight

- The DSL has strategic oversight of the Prevent Duty and online radicalisation risks, including incidents arising from AI-generated or synthetic extremist content, supported by the ICT Manager (technical controls) and SLT (policy/governance).
- This section should be read alongside:
 - Safeguarding Policy: “Radicalisation and Extremism” and Section 12 (Filtering & Monitoring; AI)
 - Online Safety Policy Section 14 (Filtering & Monitoring) and Section 10 (AI and Emerging Technologies).
- Governors receive termly updates on Prevent related online safety incidents via the Headteacher’s report.

11.2 Risk Assessment (including online)

- We conduct an annual Prevent risk assessment that considers: local threat picture; curriculum needs; pupil cohort (including SEND and vulnerable learners); device access; and online vectors (social media, gaming, encrypted apps, streaming, forums, algorithmic recommendation loops).
- Findings inform filtering/monitoring sensitivity and staff training priorities.
- Where relevant, we consider the risk that misinformation, disinformation and conspiracy theories may be used to influence pupils’ worldviews (KCSIE 2025).

11.3 Curriculum and Education

- Through ProjectEVOLVE (mapped to Education for a Connected World), PSHE/RSE, and Computing, pupils learn to:
 - recognise grooming/recruitment tactics and echo-chambers;
 - critically question content and AI-generated media (deepfakes/synthetic propaganda);
 - challenge hateful narratives and uphold respectful dialogue;
 - report concerns safely.
- Curriculum content is adapted for vulnerable learners and pupils with SEND

11.4 Filtering, Monitoring and Alerts

- Our filtering and monitoring strategy is configured to block extremist and terrorist material and to surface concerning searches/phrases for the DSL via our monitoring solution (e.g., Smoothwall), with immediate phone alerts for priority categories.
- Any filtering/monitoring failure is treated as a safeguarding incident and escalated to the DSL and ICT Manager for remediation and review.
- Provision is reviewed at least annually (and after incidents), in line with DfE Filtering & Monitoring Standards.

11.5 Staff Responsibilities and Training

- All staff receive annual Prevent awareness training, including online radicalisation indicators, escalation routes, and the limitations of filtering (e.g., 3G/4G/5G on personal devices).
- Staff are briefed on AI related risks (e.g., synthetic extremist content) and the requirement to verify online material before use in class.
- The DSL/Deputy complete Prevent/Channel updates at least annually and share local threat context in briefings.

11.6 Recognising Concerns (Online Indicators)

Staff remain alert to:

- persistent engagement with extremist narratives, including conspiracy led content or sudden shifts in online activity/language;
 - affinity with extremist influencers, groups or channels;
 - encrypted or anonymised communication patterns that evade oversight;
 - attempts to bypass filtering or access blocked content;
 - use or sharing of deepfakes/synthetic media that promote hatred or violence.
- Report immediately to the DSL; record on CPOMs.

11.7 Referral Pathways (Prevent and Channel)

- The DSL assesses concerns and, where appropriate, makes a Prevent/Channel referral to local partners (see Safeguarding Policy Appendix 4 for contact details), following Channel Duty Guidance.
- We work with police and local authority partners to assess risk and agree proportionate support; we continue to support the pupil in school throughout.
- Parents/carers are engaged where safe and appropriate; information sharing follows KCSIE and information sharing principles.

11.8 Records, Reviews and Governor Reporting

- All Prevent related online safety concerns (including monitoring alerts) are logged on CPOMs and linked to the pupil's safeguarding chronology.
- The DSL analyses patterns/trends and includes Prevent data in termly governor reports and the annual safeguarding report, informing risk assessment and curriculum planning.

11.9 Engagement with Parents/Carers

- We share weekly *Wake Up Wednesday* updates via the school app (National College) and run annual online safety/Prevent awareness workshops to help families recognise risks (e.g., algorithmic radicalisation, false information, encrypted apps) and configure device safety.
- Parents/carers are encouraged to contact the DSL with any concerns.

11.10 Links to Related Policies

- Safeguarding Policy (Sections 3.6, 12, Radicalisation & Extremism; Appendices with local contacts)
- Behaviour Policy, AUPs, Mobile Devices Policy, Data Protection, AI & Emerging Technologies (Section 10) and Filtering & Monitoring (Section 14).

12. Responding to Misuse

This section sets out how the school responds when pupils, staff, volunteers or visitors misuse ICT systems, internet, devices or online platforms, whether on-site or off-site where conduct impacts school or pupil welfare. It also covers filtering/monitoring failures and handling electronic devices that may contain harmful or illegal material.

12.1 Detection and Monitoring

- The school uses Smoothwall monitoring software to detect most misuse.
- Smoothwall provides real-time alerts for concerning searches or content, including screenshots, device ID, username, and timestamp.
- Priority alerts (e.g., suicidal ideation, extremist material) trigger an immediate phone call to the DSL.
- Termly monitoring reports are shared with governors as part of the Headteacher's report.

12.2 Immediate Actions

1. Stop the activity and make the situation safe.
2. Preserve evidence and do not view or copy indecent images of children; do not delete material.
3. Escalate to DSL (or Deputy) immediately; log on CPOMs.
4. DSL assesses risk and decides safeguarding response, including police/LA referral if required.

12.3 Pupil Misuse

- Managed under Behaviour Policy and safeguarding procedures.
- DSL considers vulnerability, intent, harm, and applies proportionate sanctions.
- Parents/carers informed where appropriate and safe.
- External referrals (police, social care, Prevent/Channel) made for illegal or high-risk activity.

12.4 Staff/Volunteer Misuse

- Report immediately to Headteacher and DSL.
- Investigated under Staff Code of Conduct and disciplinary procedures.
- Refer to LADO/police if harm threshold met.

12.5 Filtering/Monitoring Failures

- Report any failure to DSL and ICT Manager immediately.

- Contain and block access; review filter settings.
- Log incident and include in termly governor report and annual filtering review.

12.6 Handling Devices

- Searches only by authorised staff, proportionate and recorded.
- Do not view indecent images; secure device and inform DSL.
- DSL follows UKCIS guidance and police referral protocols.

12.7 Recording and Learning

- All incidents logged on CPOMs and linked to safeguarding chronology.
- Review patterns/trends; update AUPs and curriculum (e.g., ProjectEVOLVE strands).
- Report themes in Headteacher's termly report and annual safeguarding review.

12.8 Incident Categories

- Attempted bypass/technical misuse
- Harmful/illegal content access or sharing
- Cyber-bullying/harassment/discrimination
- Nudes/semi-nudes sharing
- Fraud/phishing/scams
- Extremism/radicalisation indicators
- AI-related misuse (deepfakes, unsafe prompts)
- Filtering/monitoring failure
- Device search/confiscation carried out

13. Training

- All staff: online safety at induction and annually, including current risks (AI, disinformation, scams), filters/monitoring and reporting protocols.
- DSL/Deputy: safeguarding training annually plus regular updates; lead on filtering/monitoring understanding.
- Governors: safeguarding and online safety training aligned to KCSIE and DfE standards.
- Training content draws on DfE/UKCIS materials (including Teaching online safety, harmful challenges/hoaxes, Education for a Connected World).

14. Filtering & Monitoring

The school has robust filtering and monitoring systems in place to protect pupils and staff from harmful or inappropriate online content, while enabling access to a broad and balanced curriculum. These systems are reviewed regularly to ensure compliance with DfE Filtering and Monitoring Standards (2025) and statutory safeguarding guidance (KCSIE 2025).

14.1 Filtering

- Internet access in school is filtered to block illegal, harmful, or inappropriate content, including:
 - Extremist or radicalising material.
 - Pornography and sexually explicit content.
 - Sites promoting violence, hate speech, gambling, or scams.
- Filtering is age-appropriate, balancing safeguarding with educational needs.
- The school works in partnership with IT@Trafford, who provide technical support and expertise to maintain and update filtering systems.

- Filtering settings are reviewed at least annually and after any significant incident or change in technology.

14.2 Monitoring

- The school uses Smoothwall monitoring software to detect and report concerning online activity on school devices and networks.
- Smoothwall provides:
 - Real-time alerts for high-risk searches or content (e.g., suicidal ideation, extremist material).
 - Detailed logs including username, device ID, timestamp, and screenshots.
 - Immediate phone alerts to the DSL for priority categories.
- Monitoring reports are reviewed by the DSL and ICT Manager and shared with governors termly as part of the Headteacher's report.
- All alerts are logged on CPOMs and linked to safeguarding records.

14.3 Roles and Responsibilities

- DSL: Oversees filtering and monitoring strategy, responds to alerts, and ensures safeguarding actions.
- ICT Manager: Maintains technical systems, liaises with IT@Trafford, and implements updates.
- Governors: Ensure compliance with DfE standards and receive regular reports on filtering and monitoring effectiveness.

14.4 Escalation and Failures

- Any filtering or monitoring failure is treated as a safeguarding incident:
 - Report immediately to DSL and ICT Manager.
 - Contain and block access.
 - Review and remediate settings.
 - Log incident and include in termly governor report and annual review.

14.5 Linked Policies

- Safeguarding Policy (Section 12: Safer use of internet and digital technology).
- Behaviour Policy, Acceptable Use Policies, AI and Emerging Technologies (Section 10), Prevent Duty (Section 11).

15. Monitoring Arrangements

- Behaviour and safeguarding issues related to online safety are recorded via CPOMS and alerts (e.g., monitoring software) and reviewed regularly by DSL and SLT.
- The policy is reviewed annually (or sooner if guidance changes), supported by an online safety risk assessment and a filtering/monitoring review

16. Links with Other Policies

This policy is linked to our:

- Child Protection and Safeguarding Policy (including Prevent)
- Behaviour Policy and Anti-Bullying Policy (including cyber-bullying)
- Data Protection and Privacy Notices
- Staff Code of Conduct and Safer Working Practice
- Mobile Devices/Phones Policy (DfE 2024)

- Acceptable Use Policies (AUPs) for pupils, parents/carers, staff, volunteers, governors and visitors

Appendix I – All Parents / Pupils

School Acceptable Use Agreement (AUA)

For Pupils and Parents/Carers (EYFS – Year 6)

1. Why we have this agreement

In our school technology is an important part of learning. Pupils use a range of devices including iPads in EYFS and Year 1 and individual Chromebooks from Year 2 to Year 6. This agreement helps pupils understand how to use technology safely responsibly and respectfully. Parents and carers are asked to read this with their child and sign to show that they understand and agree with our expectations.

2. Pupil Acceptable Use Agreement

When I use technology in school I will

- Be Safe
- Keep my personal information private such as my full name address passwords or phone number
- Tell an adult if I see something online that makes me worried uncomfortable or upset
- Only use websites apps and tools that my teacher has allowed
- Be Responsible
- Look after my device carefully and carry it safely
- Use my device as instructed and for learning not for games messaging or videos unless my teacher says it is allowed
- Only use my own login details and keep my passwords secret
- Be Respectful
- Treat others kindly online and offline
- Use technology in a thoughtful way with no teasing inappropriate messages or unkind behaviour
- Ask permission before taking photos audio or video of other people
- Use Devices Properly
- Follow the school rules about how iPads and Chromebooks should be used
- Not change settings install apps or try to get around filters or restrictions
- Make sure my work is my own and not copied from others or the internet

3. Parent or Carer Agreement

- The school provides filtering monitoring and supervision but no system is perfect
- My child will be taught how to use technology safely and responsibly
- I will support the school approach to online safety at home
- I will encourage my child to speak to a trusted adult if they see or experience anything online that concerns them

- I understand that school devices including Chromebooks remain the property of the school and their use may be checked or monitored for safety reasons

4. Signatures

Pupil Name: _____

Class: _____

Parent or Name: _____

Parent or Signature: _____

Date: _____

Appendix 2 – Staff, governors, volunteers and visitors - ICT Acceptable Use

Brooklands Primary School – ICT, Digital and AI Acceptable Use Declaration **(Staff, Governors, Visitors & Volunteers)**

This declaration sets out the standards expected when using the school's networks, devices, internet connection, cloud platforms and digital systems (including AI tools), both on-site and remotely. It applies to all staff, governors, contractors, visitors and volunteers. Read it alongside the school's Online Safety, Safeguarding/Child Protection, Data Protection, Behaviour, Whistleblowing and Disciplinary policies.

1) Scope and key principles

- Safeguarding first: online safety is part of safeguarding. Follow Keeping Children Safe in Education (KCSIE) and school procedures.
- Professional conduct: act lawfully, ethically and respectfully online; your behaviour reflects on the school.
- Data protection: comply with UK GDPR and the Data Protection Act 2018; only access, use and share personal data when authorised.
- Security by default: use strong passwords, MFA where provided, lock screens, report suspected incidents immediately.
- Transparency: declare when AI has materially assisted in creating content for external audiences; always apply human oversight.

2) Accounts, passwords and access

- Keep credentials secret; do not share accounts or MFA tokens.
- Use long, unique passwords (e.g., three random words) or a school-approved password manager. Change any suspected-compromised password immediately.
- Enable and use multi-factor authentication (MFA) on school systems when available.
- Only access systems and data you are authorised to use; least-privilege applies.

3) Devices and Bring Your Own Device (BYOD)

- Use school devices where possible. Personal devices may only be used for school work with prior approval and must have a passcode/biometric lock, full-disk encryption and up-to-date security patches.
- Store school data only in approved locations (e.g., [M365/Google Workspace]); do not store pupil data in personal cloud accounts.

- Do not install unlicensed, unapproved or risky software. Do not attempt to bypass filtering/monitoring.
- Physically protect devices; never leave logged-in devices unattended; lock screens when away.

4) Email, messaging and social media

- Use school-provided email and platforms for school business. Do not use personal accounts with pupils or parents/carers.
- Maintain a professional tone; communications may be disclosed under data protection or FOI laws.
- Do not create or join social media groups with pupils on personal accounts; follow the school social media policy.

5) Responsible use of AI (staff, governors and approved contractors)

- Only use AI tools approved by the school (see Appendix 5). Do not input personal data, sensitive information, identifiable pupil work or copyrighted material unless a DPIA and contract are in place and authorised.
- AI must augment, not replace, professional judgement. You are responsible for the accuracy, appropriateness and legality of AI-assisted outputs.
- Do not direct pupils to use AI tools unless explicitly permitted, supervised and age-appropriate; follow filtering/monitoring and curriculum guidance.

6) Safeguarding and online safety

- Immediately report any online safety concern about a child to the DSL (or deputy). If an adult is involved, report to the Headteacher as per policy.
- Only use approved platforms for remote learning; no private 1:1 communications with pupils outside school systems; no secret recordings or screenshots.

7) Filtering, monitoring and privacy notice

- The school operates web filtering and device/user activity monitoring to safeguard users, fulfil statutory duties and protect systems. Usage may be logged and reviewed. There is no expectation of privacy when using school systems or connections. Personal use, where permitted, must be reasonable and comply with this declaration.

8) Data protection and records handling

- Only collect the minimum personal data needed for your role and keep it accurate and up to date.
- Use official storage; apply access controls and retention schedules. Use encrypted transfer when sending sensitive data.
- Do not email spreadsheets of pupil data to personal accounts. Use secure portals when sharing externally.
- Report any data breach or loss (including misdirected emails or lost devices) immediately to the DPO and follow incident procedures.

9) Prohibited behaviour (non-exhaustive)

- Accessing, creating, storing or sharing illegal, pornographic, extremist or discriminatory material.
- Bullying, harassing or abusing others; bringing the school into disrepute.
- Attempting to bypass security, escalate privileges, access accounts, data or systems without authorisation.
- Copying or using unlicensed software or content; breaching copyright or IP when using AI or other tools.

10) Visitors & volunteers – quick rules (read before access)

- Use only the temporary/guest account or device provided. Do not attempt to access pupil records unless explicitly authorised.
- Do not take photos, videos or recordings of pupils or staff on personal devices. Follow staff directions regarding images and confidentiality.
- Report any safeguarding concern immediately to the DSL or a member of staff.

11) Compliance and consequences

- Breaches may lead to removal of access, disciplinary action (up to dismissal), termination of contracts, referral to the LADO, DBS and/or the police.

Declaration and signature

I have read, understood and agree to follow this Acceptable Use Declaration and related policies. I understand my responsibilities for safeguarding, data protection, cyber security and the responsible use of AI.

For staff/governors/contractors

Name: _____ Role/Capacity:

Organisation (if visitor/contractor): _____

Signature: _____ Date: ____ / ____ / ____

For visitors/volunteers (if different on the day)

Name: _____ Role/Capacity:

Organisation (if visitor/contractor): _____

Signature: _____ Date: ____ / ____ / ____

Reviewed: [Month YYYY] Next review: [Month

Appendix 3 – Online Safety Incident and Monitoring Log - Template

School:

Academic Year:

DSL:

System(s) Involved: (e.g., Smoothwall, CPOMS, Google Admin, IT@Trafford)

Date & Time of Incident / Alert	
Name(s) of Pupil/Staff Involved	
Year Group / Role	
Location (in school / offsite / home if device monitored)	
Device / Platform	
Type of Incident	
Description of Incident	
How Incident Was Identified	
Immediate Action Taken	
Safeguarding Level	
DSL Actions	
Reporting Route	
Outcome / Follow-Up	
Further Monitoring Required?	
Date Closed	
Recorded By	
DSL Sign-off	

- ☐ Staff must not view indecent images of children — secure the device and contact DSL immediately.
- ☐ All incidents must be recorded on CPOMS with full chronology.
- ☐ Filtering/monitoring failures are safeguarding incidents and must be escalated.

- ☐ Any Prevent-related concerns must be logged and considered for Channel referral.
- ☐ Monitoring logs feed into the Headteacher's termly report to governors.

Appendix 4 – Filtering & Monitoring Annual Review Template

Field	Details
School Name	
Academic Year	
Review Date	
Completed By (DSL)	
Completed By (ICT Manager)	
Governor Reviewer	

Field	Details
Filtering Provider	
Monitoring Provider	
Devices Covered	
Networks Covered	
Any uncovered devices/networks?	

DfE Standards – Governance & Roles

Field	Details
Roles assigned	
Governors receive termly reports	
Annual review documented	

DfE Standards – Filtering

Field	Details
Harmful content blocked	

Age-appropriate filtering	
Filtering reviewed	
Bypass requests logged	
BYOD filtering appropriate	

DfE Standards – Monitoring

Field	Details
Monitoring active on all devices	
Real-time alerts configured	
DSL receives alerts	
Monitoring detail available	
Age-appropriate monitoring	

DfE Standards – Technical Security

Field	Details
Systems updated	
Malware protection	
Secure configuration	

Incident Analysis (12 months)

Field	Details
Harmful content	
Cyber-bullying	
Nudes/semi-nudes	
Self-harm content	
Prevent/extremism	
AI misuse	
Filtering failures	
Bypass attempts	

Technical Review (ICT Manager)

Field	Details
Filtering rules updated	
Block/allow lists reviewed	
Monitoring performance checked	
Alert accuracy tested	
Account/password audit	
Device configuration audit	

Safeguarding Review (DSL)

Field	Details
Staff awareness	
Staff training	
Curriculum coverage	
SEND/vulnerable support	
AI literacy & misinformation taught	

Parent & Community Engagement

Field	Details
Safety info shared	
Parent workshop	
Website updated	

Action Plan

Field	Details
Priority	
Action Required	
Lead	
Deadline	
Status	

Final Sign-Off

Field	Details
DSL	
ICT Manager	
Safeguarding Governor	
Headteacher	

Appendix 5 – Secure AI Providers

Based on sector guidance (DfE policy paper, SWGfL AI Policy Template, and Education Data Hub recommendations), these providers are typically considered *suitable* **when used under the right conditions** and **without inputting personal data**:

Microsoft Copilot (formerly Bing Chat) – when used in an education/M365 environment

- Designed to integrate with Microsoft 365 and schools' existing security.
- Can be restricted to staff accounts; enterprise/Edu versions offer stronger data protection controls.
(DfE policy recognises mainstream tools like Copilot as examples of generative AI)

Google Gemini (Education accounts)

- Works within Google Workspace for Education environment used in many UK primaries.
- Admin controls allow schools to disable pupil access, restrict usage, and manage data retention.
(DfE references mainstream generative AI tools incl. Google Gemini)

AI tools embedded within platforms already used by schools

Such as:

- Microsoft Reading Progress / Learning Accelerators
- Google Classroom's AI features
- Widely-used EdTech platforms with AI assistants (e.g., Sparx, Century, Bedrock)
These are more suitable because they are built for education and tend to meet DP & safeguarding expectations.

Teacher-only content-generation tools with no personal data input, e.g.:

- Canva for Education (Magic Write)
- Adobe Firefly for Education (safer because it is trained on licensed data)
- QuestionWell / MagicSchoolAI / TeachmateAI (teacher accounts only, no pupil data input)

Appendix 6 – Prevent Risk Assessment

Risk Area	Identified Risk	Evidence / Context	Controls in Place	Risk Level
Local Threat Picture	Exposure to extremist or harmful narratives within a wider regional context	School located in Sale, Trafford, Greater Manchester — an area with recognised Prevent risks, particularly online	DSL monitors local authority and Prevent updates; risk reviewed annually	Low
Pupil Cohort & Vulnerability	Some pupils may be more vulnerable to influence due to SEND, SEMH, or communication needs	Cohort includes SEND pupils and vulnerable learners who may struggle to critically evaluate content	SEND support, trusted adults, safeguarding reporting routes, close monitoring of device use	Low– Moderate
Curriculum Offer	Pupils may lack understanding of online risks without structured teaching	National guidance highlights education as a key protective factor	Weekly online safety lessons via <i>Project Evolve</i> ; British values embedded across curriculum and in assemblies	Low
Online Vectors	Exposure to harmful content through social media, gaming, streaming, forums, or messaging apps	Children may access age-inappropriate content outside school; content often appears without deliberate searching	Filtering and monitoring systems; clear acceptable use policies; staff vigilance; parent workshops; safeguarding newsletters; Wake Up Wednesday	Moderate
Algorithmic Recommendation Loops	Repeated exposure to increasingly emotive or extreme content due to automated recommendations	Platforms amplify similar content once a pupil engages with a theme, narrowing viewpoints over time	Curriculum teaches critical thinking; parent workshops' safeguarding newsletters; Wake Up Wednesday	Moderate
Monitoring & Alerts	Risk of missed early indicators if online activity not reviewed effectively	Monitoring systems generate alerts linked to safeguarding and Prevent indicators	Alerts analysed by DSL; patterns reviewed; escalation procedures in place	Low
Referral & Escalation	Risk of delayed intervention or inappropriate thresholds	Prevent referrals previously made but did not meet threshold	Demonstrates professional curiosity and proportionate response	Low
Staff Awareness & Training	Staff may not recognise early signs of radicalisation	Prevent risks evolve, particularly online	Annual Prevent training; Prevent embedded in safeguarding induction	Low
Response to Emerging Risks	New local or national threats not identified promptly	Threat landscape changes over time	Risk assessment reviewed annually and in response to local intelligence	Low

