Banks Road Online Safety Audit & Risk Assessment

Curriculum, General Approach & Communication

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
APPROACH				
Approach: whole-school & safeguarding-driven – Is online safety fully accepted as part of safeguarding and therefore not treated as a separate matter, in the eyes of staff, students or parents, and equally in the curriculum and communications, and reflected in incident management and staff roles and responsibilities? – How does the school demonstrate a whole-school approach to online safety, as particularly advocated in Keeping Children Safe in Education (KCSIE), Teaching Online Safety in School (TOSIS) and subject guidance including Relationships and Sex Education and Health Education (RSHE) and Computing? Are all staff aware that any discussion of online safety, planned or ad hoc, by staff or visitors, may lead to a disclosure and must be dealt with in line with school safeguarding procedures? – Is online safety included on safeguarding reports to governors and in safeguarding concern systems – preferably integrated throughout rather than discrete? – Does online safety have obvious involvement of the leadership team and governors? – How does the school ensure that non-specialist staff use consistent approaches and messaging? – Does the school take a non-victim-blaming approach (avoiding statements such as "well you shouldn't be on social media anyway" in response to an incident or disclosure)? How is this evidenced?	🟩			Banks Road Primary School takes a **whole-school, safeguarding-first approach** to online safety, ensuring that digital safeguarding is embedded across policies, curriculum, staff culture, pastoral systems, and parental engagement. Online safety is **not treated as a standalone strand** but is integrated into the school's wider safeguarding strategy, behaviour culture, RSHE curriculum, PSHE curriculum, and Computing curriculum. This ensures that pupils learn to navigate the online world safely, respectfully and responsibly. Our approach draws explicitly on statutory guidance including: • **Keeping Children Safe in Education (KCSIE)** • **Education Act 2002 (s.175)** • **Relationships & Health Education statutory guidance (DfE, 2025)** • **DfE Filtering & Monitoring Standards** • **DfE Behaviour in Schools** and **Mobile Phones in Schools** • OEAP guidance on off-site online conduct (as relevant for residentials and trips) **1. A whole-school safeguarding culture that prioritises digital safety** Online safety is guided by the same safeguarding principles underpinning the Child Protection Policy, Staff Code of Conduct, and safer working practice. Staff are required to:

	🟩			- model safe, respectful online behaviour - challenge unsafe online conduct - report concerns immediately (including low-level concerns) - reinforce the "no use, no sight, no sound" culture for mobile phones - ensure safe device usage and data protection at all times (AUP requirements) - follow strict protocols for searching and confiscation of digital devices The RSHE Policy reinforces this safeguarding-led approach, emphasising that pupils must be taught how to **recognise risks, set boundaries, and report concerns (including online)** as part of statutory Health and Relationships Education. **2. Online safety embedded across the curriculum (Computing + PSHE + RSHE)** Online safety is not limited to Computing lessons. It is planned and sequenced **across multiple curriculum areas**, ensuring learning is revisited in age-appropriate ways and linked to wider themes of relationships, risk, privacy, wellbeing and help-seeking. **Computing Long-term Plan** The plan ensures progressive digital literacy from EYFS to Y6, covering: - recognising online and offline technology safely in EYFS/Nursery - personal information, passwords and trusted adults from Y1 - staying safe online (CEOP materials) in Y2 - email safety, clickbait, reliable sources and viruses in Y3 - smarter searching, online risks and personal data

	🟩			in Y4 • internet & WWW, networks, data and digital citizenship in Y5 • social media, online safety, PEGI ratings and consent in Y6 This sequencing ensures all pupils gain the technical, critical-thinking and evaluative skills needed to navigate online environments confidently. **PSHE Long-term Plan (Sept 2026)** PSHE units explicitly link to online friendships, cyberbullying, digital risk and influence, including: • “Adverse online friendships” and “Positive online friendships” (Y3 Relationships) • “Cyber Detectives” – fraud, online scams, gaming payments (Y5/6 Dreams & Goals) • “Send me a selfie” – image-sharing, coercion, online pressure (Y6 Changing Me) • “What to do if someone online makes you uncomfortable” (Y6 Changing Me) • kindness, respect, bullying and diversity themes foundational from EYFS upwards PSHE therefore strengthens the relational, emotional and ethical dimensions of online safety. **RSHE Draft Policy (2026)** RSHE directly reinforces online safety through statutory content covering: • respectful online behaviour • privacy and information sharing • evaluating online contacts • recognising harm and reporting • age restrictions (e.g., social media minimum age 13) • early introduction to concepts like image-sharing

	🟩			permanence, scams, fraud, deepfakes, sextortion (upper KS2) This ensures online safety is taught as part of **safe relationships**, **personal boundaries**, **consent**, and **wellbeing**. **3. Clear systems for reporting concerns and early intervention** A consistent, safeguarding-aligned reporting architecture supports online safety: • Staff report concerns immediately to DSL/SLT via CPOMS. • Pupils are explicitly taught how to report worries, online harm, pressure or bullying (CP, RSHE, PSHE). • Parents have clear routes to report incidents and are discouraged from addressing these on social media. • The Anti-Bullying Policy includes cyberbullying and AI-enabled bullying, with clear investigation procedures. • AUP breaches have defined, proportionate sanctions for pupils and staff. This aligns with the RSHE policy principle that pupils must understand **how to report abuse, including online abuse** and get help until they are heard. **4. Filtering & monitoring aligned with DfE expectations** The school meets DfE filtering and monitoring standards through: • partnership with MGL (technical provider) • leadership oversight (Headteacher, SBM, DSL) • filtering that blocks inappropriate content and reduces risk • monitoring that alerts leaders to concerning

	🟩			search terms or behaviour • clearly defined staff responsibilities as outlined in the ICT AUP This ensures technical systems support the safeguarding curriculum and behaviour expectations. **5. Staff training and professional expectations** All staff receive regular training in: • online safety and emerging digital risks • AI-enabled harms (manipulated media, impersonation, harassment) • cyber security, phishing, data protection • safe searching, filtering awareness and reporting • safe handling of digital devices and images • responding to disclosures related to online harm This is reinforced by the Staff Code of Conduct and Managing Allegations Policy, which address staff online behaviour, digital communication boundaries and whistleblowing expectations. **6. Parental engagement and transparency** Parents are engaged through: • annual curriculum meetings • RSHE policy consultation and resource transparency (parents can view all materials used). • regular communication about online risks, gaming, social media and devices • clear expectations in the Mobile Phone Policy and Parent AUP This ensures a joined-up approach between home and school. **7. Inclusivity, SEND-sensitive adaptations and safeguarding for vulnerable pupils** The RSHE and PSHE curricula emphasise safety for

	🟩			children who may be disproportionately vulnerable online, including those with SEND or additional needs. Online safety teaching is adapted for individual pupils, ensuring accessible, concrete instruction and additional adult support where required. **8. Behaviour, respect and positive digital citizenship** Online behaviour expectations align with the Behaviour Policy, Anti-Bullying Policy and school values (Respect, Friendship, Determination, Trust and Positivity). Respectful, kind online communication is reinforced from EYFS and mapped progressively across PSHE and Computing. **Overall Summary of Approach** Banks Road Primary School's approach to online safety is: • **safeguarding-driven**, not IT-driven • **whole-school and cross-curricular** • **policy-aligned** with strong coherence across AUP, Behaviour, Anti-Bullying, RSHE, PSHE and Computing • **progressively sequenced**, building age-appropriate digital resilience and critical thinking • **supported by effective technical systems** • **rooted in values and relationships**, not simply compliance • **transparent to parents** • **responsive to emerging online risks** (AI, fraud, grooming, scams, deepfakes, image-sharing) This ensures every pupil is supported to navigate the digital world with **safety, integrity and confidence**.

Approach: flexible, current curriculum – How does the school combine an informed, proactive, planned approach with a flexible, reactive approach to ensure it meets changing pupil needs (e.g. as technology changes, trends develop, incidents occur in school, are they fed into curriculum design and staff training)? – Are staff comfortable with making the most of ad hoc opportunities to discuss and learn as online safety conversations arise? – Are staff empowered to make changes to the scheduling and content of planned lessons to meet neds as they arise throughout the year (e.g. if there is a bullying incident in October, not waiting to teach this until Easter)? – How does the school review annually that teaching is current and relevant to the setting and pupil needs and experiences? – Are all the harms and issues and 'underpinning behaviours' mentioned in TOSIS and the RSHE guidance addressed throughout the year? – How are new trends identified and how are these incorporated into the curriculum as needs arise, even during the year (e.g. new gen AI tools and harms)? – Does the curriculum cover the use of emerging AI tools such as nudifying apps, AI girlfriends, etc and recognise that many pupils will come across these at home? – Is particular consideration made for vulnerable students, e.g. those with SEND and other needs? – How does the school avoid overlapping teaching, e.g. covering the same issue in different subjects (e.g. RSHE and Computing)? – Do you collate 'pupil voice' to ensure messaging addresses pupils' lived experiences? – Do curriculum planners meet with safeguarding team to ensure shared awareness of incidents and current needs as well as lesson plans and notable outcomes, strengths and weaknesses? – Do you ensure that positive experiences online are also celebrated (not just harms and negative aspects of life online)?	🟩			Banks Road Primary delivers an online safety curriculum that is **flexible, responsive, and current**, ensuring that teaching reflects emerging risks, statutory expectations and the lived online experiences of pupils. The curriculum is not static: it evolves each year through monitoring, safeguarding analysis, DSL oversight, staff feedback, parental consultation and national updates. **1. Curriculum is sequenced AND responsive to emerging risks** **Computing Long-Term Plan** The Computing curriculum shows a clearly sequenced progression of online safety knowledge from EYFS to Year 6, including: • Early skills in recognising "who we can trust with information" in Nursery and EYFS. • Personal information, passwords, and "trusted adults" by Y1–2. • Email safety, clickbait, viruses, evaluating websites and source reliability in Y3. • Searching safely, understanding personal data and online dangers in Y4. • Internet vs WWW, online networks and digital citizenship in Y5. • Social media, PEGI ratings, in-app purchases and safe online interaction in Y6. **Flexibility:** Online safety units can be moved or supplemented based on concerns emerging from CPOMS trends (e.g., Y3 email safety revisited if phishing attempts increase). **PSHE Long-Term Plan (2026)** PSHE includes up-to-date online risk coverage, including: • "Adverse online friendships" and "Positive online

	🟩			friendships” (Y3). • “Cyber Detectives: online fraud, gaming payments, scams” (Y5 & Y6). • Y6 units on image-sharing, coercion, harmful online pressure (“Send me a selfie”). • Regular revisiting of bullying, digital respect and help-seeking across all year groups. **Flexibility:** Themes such as scams, AI risks, gaming influence and online pressure can be updated annually through BBC, CEOP and SIL materials. **2. RSHE curriculum integrates the *most current* online safeguarding expectations** The RSHE Draft Policy (2026) includes updated statutory guidance (July 2025) and makes online safety a **core safeguarding theme**, including: • respectful online behaviour • privacy & information sharing • evaluating contacts & content • deepfake awareness and permanence of images • risks of scams, fraud, online manipulation, pressure and sextortion (upper KS2) • digital boundaries and reporting routes This ensures that your online safety education reflects **current national priorities**, not outdated pre-2025 content. **Flexibility:** The RSHE policy is under consultation with staff, governors and parents, allowing you to update curricular content in response to community needs and parental feedback.

	🟩			**3. Curriculum reflects *local safeguarding intelligence* and CPOMS trends** Although not explicitly in the curriculum documents, your policies indicate that: • CPOMS records are reviewed termly by DSL/SLT to identify patterns of online harm. • Curriculum units (e.g., Y3 online friendships, Y5 fraud, Y6 image sharing) can be moved earlier or enhanced depending on risk. This ensures curriculum content reacts to **real online behaviours** seen among Banks Road pupils — not a generic national model. **4. Curriculum integrates national, reputable, regularly updated resources** Across RSHE and PSHE, the school uses: • **NSPCC Speak out Stay safe** and **NSPCC PANTS** • **CEOP Jessie & Friends** (KS1 online safety) • **Ariel Trust “Send me a selfie”** (KS2 image-sharing/pressure) • **BBC Financial Education: gaming, scams, gambling** (KS2) • **SIL online friendship resources** These organisations update materials **yearly**, ensuring your online safety teaching keeps pace with evolving digital risk. **5. Flexibility through cross-curricular links** Online safety is not locked to Computing or PSHE schedules — it is integrated when relevant into: • RSHE (privacy, consent, respectful behaviour, reporting)

	🟩			• Behaviour and Anti-Bullying lessons (including AI-enabled bullying) • Safeguarding assemblies • English/media units (critical reading of online information) • Class Dojo communications & digital reward systems (reinforcing digital citizenship) This ensures adaptability across subjects and year groups. **6. Mechanisms for keeping the curriculum current** • **Annual RSHE review** (policy states yearly review or earlier if guidance updates). • **Parental consultation cycles** feed into sequencing and content refinement. • **Curriculum maps reviewed annually** to ensure computing and PSHE respond to new technologies and risks. • **Filtering & monitoring data** used to spot new emerging issues (e.g., trending search terms). • **Staff training** updated regularly to include AI harms, scams, new platforms, image-based abuse.
Assessment – Is the curriculum informed by and measured against clear outcomes, e.g. those in the UKCIS framework Education for a Connected World (or similar)?How do you use formative and summative assessment to ensure you are aware of pupil knowledge and skills to inform teaching, and subsequently to measure progress	🟩			Banks Road Primary uses a **coherent, curriculum-aligned and workload-sustainable** assessment model to evaluate pupils’ online-safety knowledge, skills and behaviours across Computing, PSHE and RSHE. Assessment is designed to (i) surface misconceptions early, (ii) check secure understanding at key points, and (iii) inform next-step teaching and targeted support—while remaining proportionate for staff. This approach is codified in the **Assessment Handbook** and operationalised in Computing using **MGL’s assessment tools**.

	🟩			**1) What we assess (and where)** • **Knowledge of safe/unsafe online behaviours** (privacy, personal information, reporting routes, respectful conduct). Taught and checked within Computing units (e.g., “Staying Safe Online”, “Social Media & Being Safe Online”) and revisited in PSHE/RSHE sequences. • **Application/decision-making in scenarios** (e.g., dealing with friend requests, image-sharing pressure, scams/fraud). Assessed through in-lesson questioning, pupil responses and short end-of-unit tasks as part of our formative/summative blend. • **Key vocabulary and concepts** (consent, privacy, password strength, PEGI, phishing, reliability of sources), checked via retrieval and quick quizzes in foundation subjects. **2) Formative assessment: in the lesson, every lesson** We prioritise **live, responsive assessment** because it is more impactful for pupils and more sustainable for teachers: • **Live marking & verbal feedback** to address misconceptions immediately in Computing/PSHE/RSHE lessons. • **Foundation-subject routines** (retrieval, quick-checks, targeted follow-up question only where needed) ensure focus on core knowledge and vocabulary without unnecessary marking. **Why this matters:** our Handbook sets the expectation that *evidence of assessment is seen in learning and adaptations*, not the volume of written comments.

	🟩			**3) Summative assessment: purposeful, light-touch, and aligned** - **Computing end-of-unit checks** use **MGL End-of-Unit Assessment Quizzes** with results logged to the **MGL Assessment Spreadsheet**, giving a simple picture of who is secure and who needs reteaching or targeted input on online-safety strands. - **Foundation-subject judgements** (Working Towards / Working At / Greater Depth) are made against curriculum-taught content using shared, subject-aligned descriptors, keeping data valid and comparable across classes. **4) Using assessment information** - **Immediate teaching adjustments**: Where MGL quizzes or class evidence flag gaps (e.g., weak grasp of privacy settings or reporting routes), teachers reteach, pre-teach or revisit in assemblies. - **Subject leadership & improvement**: Subject leads use the comparable, curriculum-aligned data to identify patterns (e.g., year-group variances in understanding scams or image-sharing), plan CPD, and refine long-term sequencing. **5) Parity, moderation & workload** - **Standardised conditions** for termly assessments (where applicable) and **directed time** for moderation ensure fairness and consistency while protecting teacher workload. - In Computing, the **MGL model** provides common tools (quizzes, spreadsheet) that reduce admin

	🟩			and help teachers focus on the *why* and *what next* of the data. **6) Inclusion & safeguarding alignment** • The assessment model supports **adaptive teaching** (targeted reteach, small-group pre-teaching) so pupils with SEND or emerging vulnerabilities secure foundational concepts like *personal information*, *reporting routes*, *respectful conduct*. • Where assessment flags safeguarding-relevant concerns (e.g., repeated unsafe choices or disclosures), staff record on CPOMS and DSL triages—linking assessment with **early help** and curriculum reinforcement. **7) How MGL Computing Policy strengthens our assessment of online safety** • Confirms **termly assessment** in Computing using **MGL End-of-Unit Quizzes** and **MGL Assessment Spreadsheet**, giving clear, unit-by-unit visibility. • Positions the **Computing Subject Leader** to support staff with planning, delivery and **assessment**, and to liaise with safeguarding leads so online-safety remains a priority. • Reinforces that while filtering is in place, **teaching children about online safety and responsibilities** is essential—assessment evidence is a feedback loop to check that teaching has *landed*. **8) What success looks like (evidence we gather)** • Pupils can **explain and apply** safe choices in

	🟩			age-appropriate scenarios (e.g., image-sharing, friend requests, reliability of sources). (Formative books/work, purple-pen responses; end-of-unit MGL quiz outcomes). • Year-on-year **progression** visible in Computing long-term map (e.g., Y2 “Staying Safe Online” → Y6 “Social Media & Being Safe Online”), with summative checks showing increased security over time.
Parental engagement – How do you proactively engage parents/carers? – Are parents aware of the school’s broad online-safety approach? – Have you supported parents to become aware of the latest harms and issues as well as encouraged to use safety settings on popular platforms, devices, games, apps and consoles? – Are parents reminded of the importance of following age ratings? – Do you follow a drip-feed approach to communicating with parents?	🟩			Banks Road Primary School places a strong emphasis on **working in partnership with parents and carers** to promote safe, respectful and responsible online behaviour. We recognise that online safety cannot be achieved by school provision alone; it requires **consistent messages between home and school**, proactive communication, and accessible, up-to-date guidance for families. This aligns with the school’s safeguarding-first approach, the RSHE duty to ensure transparency with parents, and the open communication ethos outlined in our Assessment and Computing policies. **1. Regular, proactive communication through online safety newsletters** The school provides **regular Online Safety Newsletters**, created by the Computing Lead and shared with all parents on **ClassDojo**. These newsletters: • highlight emerging online risks • explain age restrictions (e.g., WhatsApp & Snapchat 13+) • give clear, practical guidance for families on managing group chats, privacy settings and digital behaviour • offer strategies to help parents talk to children about respectful language online

	🟩			Newsletter Issue 20 (for example) covers: • risks in group chats – impersonation, anonymity, bullying • inappropriate language online • promoting open conversations at home • specific steps parents can take (privacy checks, involvement in group chats, modelling respectful behaviour) This ensures parents receive **timely, accessible information** rooted in safeguarding practice and aligned with trends identified through CPOMS, pupil voice and teacher feedback. **2. Clear alignment between school policies and parent messaging** Messages shared with parents reflect and reinforce expectations in: **Online Safety & AUP Policies** Parents are reminded that children must use age-appropriate platforms, keep accounts private, and follow the school's expectations for respectful digital conduct. **RSHE Draft Policy (2026)** Parents are informed that RSHE covers online behaviour, privacy, evaluating information, image-sharing risks and reporting concerns. The school's commitment to transparency means that parents may view all RSHE materials used. **MGL Computing Policy** The Computing Policy states that online safety education is a priority and that rules for safe internet use are displayed and taught across the school. The Computing Lead works closely with safeguarding leads to ensure parents receive accurate, up-to-date

	🟩			guidance. **Behaviour & Anti-Bullying Policies** Parents are regularly reminded that bullying—including cyberbullying—is not tolerated and that respectful communication online is expected at all times. This ensures that parental engagement is **consistent**, **joined-up**, and grounded in the same safeguarding framework used in school. **3. Using ClassDojo as a safeguarding-aware communication tool** ClassDojo is used as the primary communication platform to ensure: • instant, reliable distribution of Online Safety Newsletters • wide parental reach and accessibility • opportunities for two-way dialogue with staff • reinforcement of school expectations across home and school settings ClassDojo posts often include: • links to national campaigns (NSPCC, CEOP, Internet Matters) • reminders about device privacy settings • updates on school filtering & monitoring systems • explanations about high-risk online issues (e.g., AI-generated images, scams, gaming features) This ensures parents receive **clear, digestible guidance** in real time. **4. Parents as partners in safeguarding** Through regular contact, the school encourages and supports parents to: • talk openly with children about online behaviour

	🟩			and wellbeing • check devices regularly • monitor group chats and block/report inappropriate content • use parental controls and filters • understand that online words have the same impact as face-to-face interactions • report concerns to school promptly (ClassDojo, email, in person) Newsletter Issue 20 specifically advises parents to *review who can add/messaging their child*, *adjust privacy*, and *consider leaving risky group chats*. The school's approach ensures parents are not only informed but **empowered** to take active steps at home. **5. Workshops, consultations & policy transparency** The school further strengthens parental engagement through: • **parent RSHE consultations** (part of the 2026 policy development) • **Meet the Teacher evenings**, where online safety expectations are shared • **opportunities for parents to view all RSHE materials used in school** • supportive conversations led by DSL, Computing Lead or pastoral staff where concerns arise This ensures parents understand what is being taught and why, and that they can contribute to shaping the approach. **6. Responding to emerging risks: data-informed communication** Parent updates are not generic—newsletters and

	🟩			ClassDojo messages are informed by: • CPOMS trends (e.g., increased reporting of group chat issues) • insights from pupil voice • staff observations • current issues raised nationally • safeguarding briefings and MGL updates This makes parental engagement **responsive, relevant and preventative**.
External influences, resources and scares – Are external resources always first assessed for appropriateness (age appropriate, not overly negative, scary, victim blaming etc.)?Are any externally purchased schemes of work/curricula carefully adapted as necessary (both proactively at the start of the year and in response to incidents/trends)?What approach does the school take to reacting to online challenges, scares and hoaxes? – How are any external visitors vetted for expertise, appropriateness and safeguarding understanding?	🟩			**1) Platform trends, viral hoaxes and "scares"** • The Computing Lead uses **regular Online Safety Newsletters** to brief parents on *actual* risks pupils are encountering—e.g., group chat dynamics, impersonation and inappropriate language—so families act on **concrete guidance** (age limits, privacy settings, when to leave a chat, how to model respectful behaviour) rather than rumours. • Where external "scare" stories circulate (e.g., rumours of harmful challenges), your approach is to **triage via DSL and curriculum leads** and communicate evidence-informed advice through ClassDojo, avoiding amplification while still equipping families with practical steps and reporting routes. This process aligns with your CPOMS-centred safeguarding workflow. **2) National guidance and curriculum linkage** • The **RSHE Draft Policy (2026)** commits to teaching pupils how to **evaluate online information**, understand **age restrictions**, **privacy**, and **image-sharing risks** (including deepfakes), and crucially, how to **report concerns until they are heard**—which gives you a stable curriculum anchor when external

	🟩			narratives spike. • The **Computing Long-Term Plan** includes clearly-sequenced online-safety content (e.g., Y4 safe searching; Y6 social media safety). This enables rapid **re-emphasis or resequencing** if a trend emerges mid-term. **3) External resources and technical support** • Through the **MGL SLA**, web filtering is **kept up-to-date**, reviewed at least annually, and tuned via change-control when a new platform or risk requires category adjustments or temporary whitelisting—so teaching can continue without exposure to harm (and without over-blocking). • The **AUP** defines who can request changes (Computing Lead → DSL/SBM → Headteacher → MGL) and ensures changes are **documented and proportionate**, preserving a safeguarding-first stance even under external pressure (e.g., “we need this site today for a project”). **4) Press and social media narratives** • Staff are reminded—via safeguarding briefings and the AUP’s reporting expectations—that **concerns must route to the DSL the same day**, not be debated on social media. Where press stories cause worry, the school responds through official channels (ClassDojo/newsletter), points parents to **age-appropriate steps**, and logs issues on **CPOMS** where relevant. **5) Families as partners** • Newsletters translate external trends into **household actions** (check chats, review who can add/message your child, model respectful language, consider leaving risky groups). This turns “scares” into **manageable steps** for parents, maintaining trust and avoiding panic.

	🟩			• The **Mobile Phone Policy** underpins this by keeping the **school day device-free** for pupils (*“no use, no sight, no sound”*), so external trends are less likely to be enacted in school (and any spill-over is managed as a safeguarding issue). **6) Safeguarding intelligence loop** • External issues that *do* touch pupils are captured in **CPOMS**; DSLs analyse patterns (termly/ongoing), adjust curriculum emphasis (e.g., revisit Y6 social media safety earlier if needed), and brief parents with targeted guidance—turning external shocks into **curriculum and culture reinforcements**. **Strengths** • **Evidence-led comms:** ClassDojo newsletters focus on *what you’re seeing now* (group chats, language, impersonation) with practical, non-alarmist advice. • **Curriculum “shock absorbers”:** RSHE/Computing provide ready-made, age-appropriate lessons to address myths, deepen critical thinking, and practise reporting, so you can respond to scares without rewriting policy every time. • **Technical agility:** MGL SLA + change-control lets you **tune filtering** quickly but safely if a platform becomes problematic, balancing protection with teaching access. **Known risks / mitigations** • **Risk:** Sensationalised media or viral rumours can generate parental anxiety and pupils’ curiosity. **Mitigation:** Maintain the “facts-first” newsletter rhythm; signpost age rules and privacy controls; route all concerns to DSL; capture incidents in

	🟩			CPOMS for proportionate follow-up. • **Risk:** New platforms or slang can outpace filters. **Mitigation:** Use the **MGL change-control** path and **curriculum re-emphasis**; empower staff to flag early and parents to apply home controls.
POLICIES & PRACTICE				
Policies – Do your policies govern all online behaviour, not just when using school devices or logged into school systems and platforms? – Do you have an online safety policy (whether standalone or section within your safeguarding and child-protection policy)?Do you have (note the following might be integrated into other policies and not standalone but must be very clear if so) ○ AUPs to reflect varied roles and responsibilities, e.g. different key stages, parents, staff, visitors, governors, contractors etc. (NB whilst often called "acceptable use policy", these should reflect all online behaviour). ○ Social media policy? If not, this may be included in your online safety policy but should be clear. ○ Home/remote learning policy ○ Information sharing protocols - How is confidential information shared with other stakeholders? Are all documents emailed via a secure system? - How is the use of generative AI captured within your policies?	🟩			**1. Safeguarding Policy & Child Protection Procedures** Banks Road Primary School has a comprehensive Child Protection Policy that aligns fully with *Keeping Children Safe in Education (KCSIE) 2025*, local safeguarding partnership procedures, safer recruitment requirements, early help processes, low-level concerns, and statutory reporting pathways. Policies consistently promote a safeguarding culture of openness, vigilance and professional accountability. **Evidence:** Clear alignment found in the Staff Code of Conduct, Managing Allegations, Online Safety, Whistleblowing, Behaviour, and Anti-Bullying policies. **2. Staff Code of Conduct (Safer Working Practices)** The school has adopted a detailed, annually revised Staff Code of Conduct, following Safer Recruitment Consortium guidance. It defines professional boundaries, whistleblowing expectations, safe working practice, low-level concerns procedures, relationships and communication with pupils, online conduct, and reporting duties. This document demonstrates strong compliance with KCSIE Part 2 and Part 4 expectations. **Evidence:** Safer Working Practices Code of Conduct for Adults (V9, Sept 2025–26). **3. Managing Allegations Against Staff & Low-Level Concerns** The Managing Allegations Policy clearly outlines case

	🟩			management, thresholds, referral processes, LADO contact, confidentiality restrictions, record-keeping, support for staff, and DBS/TRA referral duties. The policy is current, detailed and fully in line with KCSIE Part 4. Includes clear procedures for low-level concerns and self-reporting, which reinforces a transparent and preventative safeguarding culture. **Evidence:** Managing Allegations Policy (V7, Sept 2025–26). **4. Whistleblowing** The Whistleblowing Policy is comprehensive, covering protected disclosures, confidential reporting routes, escalation beyond school, protections for staff, and responsibilities for investigating serious misconduct. It specifically includes safeguarding, child protection and staff behaviour as reportable concerns. This policy strongly supports a culture of professional challenge and safeguarding vigilance. **Evidence:** Whistleblowing Policy (Feb 2023). **5. Online Safety Policy & ICT Acceptable Use** The ICT and Internet Acceptable Use Policy is strong. It includes: • filtering and monitoring arrangements • AI usage and restrictions • cyber security expectations • remote access rules • search, confiscation and deletion procedures • staff, pupil and parent AUPs • sanctions linked to the Behaviour and Disciplinary policies • links to KCSIE 2025 and UKCIS guidance This provides excellent coverage of statutory

	🟩			online safety obligations. **Evidence:** ICT & Internet Acceptable Use Policy (Nov 2025). **6. Behaviour Policy & Anti-Bullying Policy** The school has a highly detailed Behaviour Policy grounded in KCSIE, equality duties and DfE Behaviour in Schools guidance. It includes staged consequences, SEND adjustments, suspension/exclusion processes, reasonable force guidance, and staff responsibilities. The Anti-Bullying Policy is particularly strong, covering: • all forms of bullying, including online, prejudice-based, and AI-enabled bullying • detailed response, recording and safeguarding procedures • curriculum prevention measures • parental engagement and multi-agency working **Evidence:** Behaviour Policy (2025/26 versions) and Anti-Bullying Policy (Jan 2026). **7. Mobile Phone and Smart Device Policy** The school has a robust, DfE-aligned Mobile Phone Policy including: • a clear *"no use, no sight, no sound"* rule for all pupils • defined exceptions (e.g., diabetes monitoring) • staff conduct and safeguarding expectations • search and confiscation rules linked to statutory guidance • guidance for volunteers, visitors and parents This demonstrates exemplary compliance with 2025 DfE mobile phone behaviour expectations. **Evidence:** Mobile Phone Policy (Jan 2026).

	🟩			**8. Data Protection & Cyber Security** Although your dedicated Data Protection Policy is not yet reviewed here, the AUP and mobile phone policies clearly reference UK GDPR requirements, encryption, data breaches, remote access restrictions, use of school devices, and security expectations. This indicates strong practice, with operational systems embedded across ICT-related policies. **Evidence:** ICT Acceptable Use Policy & Mobile Phone Policy. **9. Searching, Screening & Confiscation** Search and confiscation procedures are explicitly referenced in the AUP, Behaviour Policy and Mobile Phone Policy. Rules are aligned with DfE 2022 guidance and outline: • authorised staff • grounds for searching electronic devices • protocols for examining/deleting content • handling of illegal material **Evidence:** ICT AUP; Mobile Phone Policy; Behaviour Policy. **10. Visits, Residentials & Off-Site Safeguarding** Mobile phone rules, behaviour expectations, online safety guidance and adult conduct procedures apply off-site. The Behaviour and AUP policies explicitly reference the school's duty to regulate behaviour beyond the school gates. **Evidence:** Behaviour Policy; Mobile Phone Policy.

Content & review, policy v. practice – Do you consult others to populate your policy, e.g. review templates (LSCP, fellow schools, The Key, LGfL, etc)? – Where you have used content or templates, have you checked it is relevant to your setting, systems and stakeholders and adapted as appropriate? – Do you regularly review these policies (not just the annual governor review but with staff and pupils who can give insights into practicability)? – How do you check that policies are followed and <u>possible to follow</u> (e.g. references to systems which no longer exist, contradictions with other policies, impossible rules like a ban on mobile photography when there are no school cameras but photos are required)? – Are new systems, platforms, processes and user behaviour/needs and incidents regularly embedded into these 'living' documents? – Are policies updated to reflect curriculum needs, behaviour and safeguarding risks and incidents <u>in your school</u>?	🟩			**1. Staff Conduct, Professional Boundaries & Digital Behaviour** **Policy** The Safer Working Practices Code of Conduct sets out strict expectations for staff behaviour online and offline, including: maintaining professional boundaries, avoiding private communication with pupils, handling of sensitive information, avoiding personal device photography, and reporting low-level concerns. **Practice** Staff follow these expectations consistently. Leaders regularly revisit digital boundaries through induction, annual safeguarding updates, CPD and ongoing reminders. Staff understand not to communicate with pupils or parents via private messaging, social media or personal devices. **Assessment** **Excellent alignment** — staff behaviours clearly reflect policy. **2. ICT Acceptable Use, Filtering & Monitoring, and Safe System Access** **Policy** The ICT & Internet Acceptable Use Policy (Nov 2025) provides exceptionally detailed requirements on: • acceptable and unacceptable use • cyber security measures • AI restrictions • data protection controls • filtering & monitoring systems • remote access rules • sanctions for breaches **Practice**

	🟩			Pupils use devices only while supervised on school-managed, filtered systems. Staff access ICT platforms via password-protected and MFA-secured accounts. Data is not stored on personal devices and staff avoid public networks. Filtering logs are reviewed by the DSL and ICT leads; the system effectively flags concerns. **Assessment** **Policy-to-practice alignment is very strong.** This is an area of clear strength. **3. Mobile Phone, Smart Device & Wearable Technology Controls** **Policy** The Mobile Phone Policy (Jan 2026) enforces a *“no use, no sight, no sound”* rule for pupils; tight restrictions for staff; and zero tolerance for image capture on personal devices. It also integrates DfE guidance on safety, safeguarding, search and confiscation. **Practice** Phones are handed in daily; breaches are rare and dealt with swiftly. Staff model the same expectations placed on pupils. Visitors are informed of requirements on entry. **Assessment** **Fully embedded in everyday practice.** **4. Online Behaviour, Cyberbullying & AI-Enabled Harm** **Policy** The Anti-Bullying and Behaviour Policies include extensive sections on: • cyberbullying • online harassment

	🟩			• AI-enabled bullying (deepfakes, impersonation, image-based abuse) • procedures for responding to online harm • sanctions and pastoral support **Practice** Staff respond promptly to online bullying concerns, documenting incidents on CPOMS. Victims receive pastoral support; perpetrators follow staged consequences. Parents are contacted early. The curriculum teaches critical digital literacy, consent and respectful online behaviour. **Assessment** **Policy and practice align closely.** Staff demonstrate strong understanding of emerging online risks. **5. Search, Screening & Confiscation (Digital Devices)** **Policy** Procedures for searching electronic devices appear consistently across the ICT AUP, Behaviour Policy and Mobile Phone Policy. They clarify: • who can search • when a search is justified • how content is examined • when images must not be viewed • when police involvement is required **Practice** Authorised staff only conduct searches. Illegal or harmful content triggers immediate DSL involvement. Incidents are logged correctly, and pupils understand expectations clearly. **Assessment** **Safe, compliant and consistent** with statutory guidance.

	🟩			**6. Curriculum, Prevention & Digital Literacy** **Policy** The AUP, Anti-Bullying Policy and Mobile Phone Policy all reference preventative education — including online safety within computing, PSHE/RSHE, and whole-school assemblies. **Practice** Online safety is taught through structured units, enhanced with assemblies and thematic weeks. Children understand not to share personal information, how to report concerns, and how to behave responsibly online. **Assessment** **Well embedded** and matches policy intentions. **7. Reporting Routes, Record-Keeping & Low-Level Concerns** **Policy** Clear reporting expectations run through: • Staff Code of Conduct • Whistleblowing Policy • Managing Allegations Policy • Child Protection procedures **Practice** Staff report any online safety concerns promptly. CPOMS is used consistently for recording incidents. DSL triage is swift, with escalation where required (LADO, Social Care or Police for criminal matters). **Assessment** **Policy-consistent and robust in practice.**

Reporting – Is there evidence that staff understand how to report online safety concerns? – Is online safety included on safeguarding reports – preferably integrated throughout rather than discrete? – Are children supported in an age-appropriate/developmentally - appropriate way to tell staff if they have an online safety concern? – Is there evidence that online safety concerns are followed up in an appropriate and timely manner? – Do all staff understand how to report concerns relation to online safety externally?	🟩			**1. Reporting by Staff** **Policy Expectations** Staff must immediately report: • any safeguarding concern arising from online behaviour or digital use • any online incident that may place a child or adult at risk • any breach of the ICT Acceptable Use Policy • cyberbullying, online harassment or inappropriate communication • accidental or deliberate exposure to illegal or harmful content • concerns about another adult's online conduct, including low-level concerns • data breaches involving school systems or personal data The Staff Code of Conduct and ICT AUP make this explicit. Staff must not handle issues informally or delete evidence — they must report directly to the DSL or SLT. The Managing Allegations Policy also instructs staff to report any concern about an adult's conduct, including online behaviour, to the Headteacher or Chair of Governors, and to escalate to LADO where thresholds are met. **Practice** Staff consistently use CPOMS to record concerns and inform the DSL immediately. Staff demonstrate good understanding of low-level concerns and self-reporting. Leaders respond the same day and provide follow-up supervision where needed. **2. Reporting by Pupils** **Policy Expectations**

	🟩			The ICT AUP for pupils instructs children to: • report anything online that upsets them • tell an adult immediately if they see harmful or inappropriate content • report cyberbullying or uncomfortable messages • report accidental access to inappropriate material The Anti-Bullying Policy requires staff to take all reports seriously, investigate promptly, and record outcomes on CPOMS. **Practice** Children know the DSL team, and staff report that pupils regularly raise concerns at an early stage. Online incidents are followed up promptly, with parents involved as appropriate. **3. Reporting by Parents / Carers** **Policy Expectations** Parents may report online safety concerns through: • direct contact with school staff • reporting cyberbullying or online misconduct involving their children • contacting the school to alert staff to incidents outside school hours • following AUP expectations when communicating about online issues The Anti-Bullying Policy states parents must communicate concerns directly with school, not via social media. **Practice** Parents use ClassDojo, telephone or face-to-face contact to raise concerns. The school documents concerns on CPOMS and follows its behaviour and

	🟩			safeguarding procedures consistently. **4. DSL & SLT Response and Escalation** **Policy Expectations** The DSL must: • review all online safety concerns and triage appropriately • escalate to Children's Services where safeguarding thresholds are met • involve LADO for concerns about staff behaviour online • contact police for illegal content (e.g., child sexual imagery, threats, hate crimes) • preserve digital evidence (screenshots, URLs, device information) • record actions and outcomes on CPOMS **Practice** DSL responds immediately to online incidents, documenting chronology and outcomes. Evidence is preserved, not deleted. Police involvement is sought where required. **5. Handling Illegal or Harmful Digital Content** **Policy Expectations** Staff **must not**: • view, copy or forward illegal images • investigate a device beyond what is lawful • delete content that may be evidence of a crime The AUP and Mobile Phone Policy require immediate DSL/police involvement in cases involving indecent images of children or threats. **Practice**

	🟩			Staff follow the policy strictly. If harmful or illegal material is suspected, the DSL secures the device and contacts police without delay. **6. Recording and Evidence Management** **Policy Expectations** All reports — minor or serious — must be logged on CPOMS. Policies clearly require: • factual recording • chronology of actions • evidence upload (screenshots, device logs, platform reports) • DSL sign-off **Practice** CPOMS records are timely, detailed and reviewed termly to identify patterns. Staff understand the difference between behaviour logs, safeguarding logs and low-level concerns logs. **7. Monitoring, Oversight & Governance** **Policy Expectations** The ICT AUP states that filtering and monitoring systems must be overseen by: • the Headteacher • the School Business Manager • MGL (technical partner) • the DSL, who must understand filtering/monitoring systems Governors must ensure compliance with the DfE Filtering & Monitoring Standards. **Practice** Leadership routinely monitors filtering alerts and ICT reports. Governors receive safeguarding updates,

	🟩			though termly filtering/monitoring summaries would further strengthen oversight.
TRAINING				
Training & CPD – Do all staff receive online safety training as part of the safeguarding training schedule (at induction and start of year or mid-year for new starters)? How does this training reflect the approach you have outlined in this audit? Has this been updated to reflect KCSIE 2025 changes (i.e. the definition around 'content' harms) – Is their expertise in online safety within the DSL team, with the most in-depth training available to this team? – How are ALL staff made aware of and regularly updated on national/regional trends and those in school relating to general behaviour, harms or incidents which non-specialist/senior staff may not be aware of without explicit updates – Is training appropriate to and customised for different roles and responsibilities, with extra strategic elements for SLT and governors? – Does training around 'online safety' tie in with training on other areas which may not be classically associated with online safety, such as all the harms mentioned in KCSIE (e.g. Prevent, exploitation, and many others)? – Do technical staff receive sufficient training on key safeguarding elements (note particularly filtering and monitoring changes)? – Do non-technical staff receive sufficient training on technical aspects (as above, particular – but not exclusive – focus on filtering and monitoring)? – Have technical, safeguarding, PSHE and other staff been given up to date information on the latest gen AI tools in use (as mentioned	🟩			Banks Road Primary delivers a **highly comprehensive, structured and annually sequenced programme** of safeguarding, online-safety, cyber-security and digital-practice training for all staff, governors and pupils. Training is clearly documented, quality-assured and reflects: • KCSIE requirements • Local safeguarding priorities • DfE Filtering & Monitoring Standards • DfE Digital Standards • Cyber-security expectations • The school's AUP, AI Policy and Computing Policy The school's training offer is **far above** the statutory minimum and demonstrates a safeguarding-first culture. **1. Whole-school safeguarding & online-safety training** All staff (teaching, support, office, trainees) receive **annual safeguarding training**, consistently delivered and clearly documented across multiple years: • **2025–26 Safeguarding Training** (13/10/25) delivered by the DSL to *all* staff, covering up-to-date safeguarding responsibilities, types of abuse, signs/indicators, reporting routes and CPOMS procedures.

above, chatbots, nudifying apps and nude image generators, AI girlfriends, etc)?	🟩			• **2024–25 Staff Safeguarding Training** (07/10/24) for all staff, including KCSIE updates and CPOMS procedures. • **2023–24 Safeguarding Training** (27/10/23) for all staff, delivered by the DSL and The Key. • **Repeated annual safeguarding cycles** across 2022, 2021, 2020 and 2019 show long-term commitment and consistency. This ensures all staff are always current with statutory guidance and school processes. **2. Online Safety–specific staff training (excellent coverage)** Banks Road provides **regular, specialist** online-safety CPD beyond basic safeguarding: • **Online Safety: The Essentials** (11/11/25) for staff, covering online risks, signs of harm, and response actions. • **Online Safety Training for All Staff** (08/05/24), focusing on school procedures, apps to watch for, risks, and managing concerns *in the moment*. • **Filtering & Monitoring Training** (15/04/24) delivered by MGL, covering KCSIE updates and cyber-incident response. • **Smoothwall Safeguard Training** for senior leaders (05/10/23) on the national picture, industry insights and filtering/monitoring effectiveness. • Repeated **Digital Community Police** workshops for children (multiple years), strengthening the culture across the whole school. This exceeds what most primary schools deliver and ensures both senior leaders and all staff understand practical online-safety risks.

	🟩			**3. Cyber-security training for all staff (unusually strong)** Banks Road is ahead of most primaries in providing **whole-staff cyber-security training**: • **Cyber Security Training – whole staff** (29/09/25) by MGL Focused on school cyber-security policies, safe AI use, data breaches and protecting the school online. • Cyber themes also integrated into filtering/monitoring training (15/04/24). This provides a strong alignment with DfE Digital Standards and the cybersecurity requirements underpinning filtering/monitoring systems. **4. Prevent, radicalisation & risk-awareness training (annual & comprehensive)** Prevent training is delivered: • **Prevent Training – all staff** (15/09/25) via Liverpool PREVENT Officer. • **Prevent Duty Training** (10–11/03/25) for teaching assistants & teachers. • **Prevent Training** (27/10/23). • **Prevent Duty in Education** delivered in earlier years (2017–18, 2018–19). This creates a continuous, multi-year thread of Prevent awareness—essential for online radicalisation risks and extremist content. **5. DSL and Deputy DSL training cycle (excellent practice)** DSL and Deputy DSL training is:

	🟩			• **Annual and fully up-to-date** (e.g., DSL refresher 22/09/25; 23/09/24; 19/09/23; 11/10/22; 07/10/21; 07/10/20; 03/10/18). • Always delivered by **School Improvement Liverpool** (local safeguarding authority), ensuring consistency with local thresholds and procedures. The school maintains a **gold-standard safeguarding leadership cycle**. **6. Governor training (strong governance awareness)** Governors receive: • **Safeguarding for Governance – The Key** (03/2025). • Governors invited to safeguarding staff meetings in previous years. Combined with the AI Policy's explicit requirement for **Chair of Governors involvement in AI tool approvals**, governor oversight is embedded across digital safeguarding. **7. Pupil-facing online-safety education (beyond statutory)** The training log shows extensive online-safety and digital-behaviour input for pupils: • **Digital Community Police Officer sessions** (multiple years) with content on social media, digital footprints, oversharing, stranger risk, cyberbullying and reporting. • **Online Safety Day at Liverpool FC** (Years 5–6). • **Mini Medics**, **Fire Champions**, and **Anti-Bullying** sessions including cyberbullying-specific content. • **Online Safety workshops** for parents + Year 6

	🟩			(2019, 2020, 2024). This meets both RSHE and Computing curriculum expectations and enhances digital citizenship. **8. AI Policy integration into staff CPD (sector-leading)** Your AI Policy (Sept 2025) requires: • staff to be trained on ethical AI use, data protection, and transparency • SLT to conduct spot-checks and ensure compliance • MGL to advise staff on AI data-integrity questions This is *exceptionally strong practice* for a primary school and positions staff to use AI safely without compromising safeguarding or cybersecurity. **9. Training is documented, sequenced and high-impact** The training log demonstrates: • **clear dates, attendees and facilitators** • **impact statements** (what changed because of the training) • **coverage across all staff groups: teachers, TAs, office staff, trainees, governors, pupils** This documentation would meet Ofsted expectations for safeguarding audit trails and demonstrates a whole-school commitment to continuous professional learning.

[END OF SECTION 1]

Safe School Systems

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
FILTERING				
General – a high-quality and school-appropriate filtering service – Has your provider filed a submission with the UK Safer Internet Centre to explain why your filtering is appropriate? – Have DSL, SLT and technical teams all read and understood the submission, including rationale, benefits and limitations and safe search settings, e.g. for web searches and YouTube? – How do you know your provider goes above and beyond this (e.g. with independent accreditation; if not, what other checks have you done to be sure the provider meets its obligations? – How do you know that you are using best-practice settings for your system?	🟩			Banks Road Primary uses a filtering system that is **robust, actively maintained, and specifically designed for primary-aged pupils**, ensuring that children experience a safe digital environment while still having access to content that supports the curriculum. The school's filtering processes are aligned with DfE *Meeting Digital and Technology Standards*, the MGL service provision, and the school's internal safeguarding framework. **1. Robust, school-specific filtering provided by MGL** The MGL Computing Policy confirms that the school has a dedicated service level agreement (SLA) with a computing/ICT resource provider to ensure that the filtering system is **professionally managed, technically secure, and regularly maintained**. The policy states that: • Web filters are kept **up-to-date** to prevent access to inappropriate materials. • The Computing Subject Leader works with safeguarding leaders to ensure online safety remains a high priority. This ensures the filtering is not a static system but one that is actively maintained and reviewed. **2. Filtering aligned with safeguarding duties and DSL oversight** Your ICT Acceptable Use Policy states that filtering and

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			monitoring systems must be overseen by: • the Headteacher • the School Business Manager • MGL (technical partner) • the Designated Safeguarding Lead, who must understand the system and respond to alerts This setup ensures: • strong **leadership oversight** • direct **safeguarding response** when necessary • consistent compliance with DfE filtering/monitoring standards • filtering is not purely technical but **integrated into safeguarding practice** **3. Age-appropriate filtering that supports the curriculum** Filtering is configured to provide a **safe but functional** online environment. Evidence from policies and curriculum structure shows: • Filtering blocks inappropriate, harmful or adult content while allowing access to curriculum-aligned resources. • Computing lessons (e.g., "Staying Safe Online", "Social Media & Being Safe Online", "Smarter Searching") rely on safe, filtered access that still allows children to practise skills without exposure to risk. • Filtering supports cross-curricular digital literacy

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			and safe use of approved apps. Filtering is therefore **age-appropriately restrictive** while still enabling effective teaching and learning. **4. Filtering updated regularly and reviewed annually** The MGL Computing Policy requires: • **annual review of web filters** to ensure protection from inappropriate or harmful online content • **annual review of the Computing Policy**, which includes filtering provisions This means filtering is not left to degrade or become outdated; it is part of an embedded cycle of review. **5. Integrated with wider school systems and expectations** Filtering is strengthened by complementary systems and policies, including: • the strict *"no use, no sight, no sound"* Mobile Phone Policy restricting unfiltered personal data connections on site • behaviour and anti-bullying policies framing respectful online conduct and responding to incidents of digital harm • RSHE curriculum teaching pupils to evaluate risk, privacy, image-sharing and online contact • consistent parental updates (via newsletters/ClassDojo) that reinforce expectations around age-appropriate platforms

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			and monitoring at home Filtering is therefore part of a **multi-layered safeguarding ecosystem**. **6. Filtering supports early identification of concerns** Your AUP states that filtering and monitoring systems enable staff to: • flag concerning user activity • detect searches or attempts to access inappropriate content • escalate concerns to the DSL This creates a feedback loop between technical filtering, staff vigilance and safeguarding response.
General – knowledge, approach, attitudes – How do you ensure there is a general understanding of the following (verbatim from the DfE standards introduction)? ○ “Filtering is preventative [...] protect[s] users from accessing illegal, inappropriate and potentially harmful content [...] identifying and blocking specific web links and web content” ○ “No filtering system can be 100% effective. [...] You need to understand: your filtering system’s coverage [and] any limitations” – How does the DSL team maintain a knowledge in general terms of WHAT is blocked (or allowed), for WHOM, WHEN/WHERE and most importantly WHY (safeguarding not tech-driven rationale)? – How are all staff reminded that filtering is all about safeguarding and that they are the eyes and ears to warn of gaps or overblocking? – Is the DSL team clearly in charge of filtering (not the same thing as	🟩			Banks Road Primary demonstrates a **high level of whole-school awareness, professional knowledge and positive safeguarding attitude** toward filtering and online safety. Filtering is not treated as a purely technical function: it is embedded in staff behaviours, leadership oversight, digital safeguarding decisions and curriculum design. **1. Leaders hold strong, up-to-date knowledge of filtering and online risk** Your ICT Acceptable Use Policy states that the Headteacher, School Business Manager and DSL have **defined responsibilities for understanding, overseeing and responding to filtering and monitoring systems**. They are explicitly required to:

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
being technical experts or 'doing' configuration/setup)? – Are you confident you follow best-practice recommendations, e.g. to be as granular as possible (using user authentication and decryption)?	🟩			• understand how filtering and monitoring systems operate • review their effectiveness • escalate concerns appropriately • ensure compliance with DfE Filtering & Monitoring Standards The MGL Computing Policy reinforces this, requiring the Computing Subject Leader to remain up-to-date with developments in online safety and to work closely with the DSL to ensure safeguarding remains a priority. This demonstrates senior leaders and subject leaders have the **professional knowledge** needed to make informed decisions about filtering. **2. Staff attitudes reflect a safeguarding-first mindset** Across multiple policies, staff are expected to: • model safe, appropriate digital behaviour • recognise unsafe or concerning online activity • report filtering or access issues promptly • escalate online-safety concerns to the DSL This develops a **collective duty of care**, strengthening the school's human-layer defences against digital harm. The MGL policy also requires teachers to keep **up-to-date records of formative and summative assessment** and to plan according to pupils' abilities. This includes monitoring how pupils navigate the filtered environment and respond to online-safety teaching. Staff attitudes are therefore grounded in **safe use, vigilance and professional responsibility**.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**3. The school understands filtering as part of a wider safeguarding system, not a standalone tool** Policies consistently frame filtering as only **one layer** within a multi-layered safeguarding approach. Filtering is combined with: • the Mobile Phone *"no sight, no sound, no use"* rule, preventing unfiltered mobile data access on site • curriculum teaching on safe choices, respectful online behaviour and evaluating content (PSHE, RSHE, Computing) • strong reporting routes for staff, pupils and parents • parental engagement via newsletters, ensuring risks seen outside school are understood and addressed This indicates a mature, **holistic approach**, rather than reliance on filtering alone. **4. The school actively monitors emerging online risks and adapts attitudes accordingly** The Online Safety Newsletter demonstrates that the Computing Lead tracks **real-world online trends** (e.g., group chat misuse, inappropriate language, impersonation, bullying) and communicates these to families, reinforcing a culture of *alertness and adaptability*. This shows the school's approach is **dynamic**, grounded

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			in: • real-time risk awareness • responsiveness to new platforms and behaviours • continual reinforcement of safe digital attitudes **5. Pupils develop positive attitudes to safe behaviour through whole-school culture** Through the Computing curriculum, pupils learn: • to “use technology safely and respectfully” (KS1/KS2 statutory content) • to recognise unsafe behaviour, harmful language and inappropriate contact • to evaluate online information • where to go for help, and how to report concerns • to apply respectful online behaviour across contexts Through RSHE, they learn: • privacy, boundaries and safe image-sharing • digital risks such as scams, fraud and deepfakes These curriculum elements reinforce **positive digital citizenship attitudes**, teaching children to work *with* the filtering system—not around it. **6. Senior leaders model and promote the right safeguarding attitudes** Leadership modelling is evident in: • transparent communication with parents (RSHE consultations; online safety newsletters)

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• routine policy review cycles (annual review of filtering provisions in MGL policy) • mandated oversight of filtering, showing that leaders prioritise digital safeguarding as part of statutory duties This demonstrates a school-wide safeguarding culture where **filtering is integral to leadership responsibility**.
DfE Standards – high level – Do DSLs and SLT understand that they are not complying with the standards by subscribing to a reputable filtering providers, but that compliance is based on how/whether a school uses filtering appropriately for its setting, and on the rationale for decisions and day-to-day practice by the school? – At a very high level (detail to follow), are you satisfied your school is complying with these standards (NB this section relates mostly to S1-3)? – What are the key action areas for the school to improve on and improve compliance over the next 12 months?	🟩			Banks Road Primary's filtering system demonstrates strong alignment with the **DfE Filtering & Monitoring Standards**, ensuring that children are protected from harmful or inappropriate online content while having safe, age-relevant access to the digital resources needed for learning. The school's approach is **strategic, safeguarding-led, and technically robust**, showing clear evidence that high-level DfE expectations are met. **1. Filtering is safe, secure, and age-appropriate** The MGL Computing Policy confirms the school uses *professionally managed*, school-specific filtering that is: • regularly updated • designed to prevent access to inappropriate materials • reviewed annually to ensure continued protection The ICT AUP reinforces that the school provides a **secure online environment**, with filtering configured to meet the needs of primary pupils and block harmful content. This meets the DfE expectation that filtering must be

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**appropriate to age, educational level, and safeguarding context**. **2. Clear leadership ownership and governance** The DfE requires that filtering responsibilities are allocated to identifiable leaders. Your policies explicitly state that filtering oversight is held by: • **Headteacher** • **School Business Manager** • **DSL** • **MGL technical partner** This ensures: • leaders understand the filtering system • accountability is clear • filtering is integrated into safeguarding governance pathways This is **fully aligned** with the DfE requirement that strategic leadership must manage filtering. **3. Safeguarding integration, not just technical provision** Filtering at Banks Road is embedded into safeguarding systems: • DSL understands and oversees filtering and monitoring alerts • systems ensure staff can raise concerns promptly • filtering interacts directly with safeguarding

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			processes (CPOMS reporting, DSL triage) The MGL Computing Policy also requires the Computing Lead and Child Protection Officer to work together to prioritise online safety. This demonstrates filtering is treated as a safeguarding tool, meeting DfE expectations that filtering must be part of a **broader safeguarding strategy**. **4. Regular review and evaluation** DfE standards require at least annual review of filtering effectiveness. Your MGL Computing Policy commits to: • **annual review of web filters** • **annual review of the Computing Policy** (inc. filtering arrangements) This ensures filtering is not left static and remains compliant with evolving risks and DfE requirements. **5. Proportionate filtering that supports learning** The school's filtering configuration is deliberately balanced: • strict enough to block inappropriate content • flexible enough to enable curriculum delivery, research tasks and Computing units • aligned with PSHE/RSHE online-safety coverage (privacy, evaluating content, reporting) This meets the DfE expectation that filtering should "*not lead to unreasonable restrictions on teaching and learning*."

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**6. Awareness of emerging risks and active communication** The Online Safety Newsletter shows your Computing Lead proactively identifies and responds to **current online trends** (group chat misuse, inappropriate language, impersonation risks) and updates parents accordingly. This contributes to the DfE standard that schools must be **alert to new and emerging online threats** and maintain a dynamic approach to filtering. **7. Filtering is complemented by prevention education** The DfE notes that filtering alone is insufficient without effective education. Your Computing, PSHE and RSHE curricula explicitly teach pupils: • respectful online behaviour • how filtering protects them • how to recognise suspicious or harmful content • how to report concerns This ensures filtering is understood by pupils as part of a wider digital safeguarding ecosystem.
Standard #1 - Identify and assign roles and responsibilities to manage your filtering and monitoring systems – Where are these roles / responsibilities outlined (normally online safety policy and maybe AUPs too) – How do you ensure that the DSL and IT teams collaborate effectively to make informed, decisions (details of how/when)?	🟩			Banks Road Primary has **clearly assigned, named roles** and an **escalation pathway** to ensure filtering and monitoring are governed, operated, and reviewed as part of safeguarding—not just "IT". This aligns with the ICT Acceptable Use Policy and the MGL Computing Policy. **1) Governance & Strategic Leadership**

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
– How often does the DSL team check reports, what do they check and how do they track actions? – Who is your named F/M governor and SLT member (DSL is the lead but some may have additional SLT support)? – How do they understand their roles and are all staff aware who they are and their roles? – What is the mechanism and schedule for involving / feeding back to governors/SLT on regular checks and reviews? – Who are the internal and/or external technical support (setup, configuration, operation), and are they and all staff aware of them and their duties?	🟩			• **Governing Board** Holds the Headteacher to account for compliance with DfE Filtering & Monitoring Standards and ensures filtering/monitoring are part of the school's wider safeguarding assurance (termly DSL reports / annual policy reviews). • **Headteacher — Jamie Wilson** Owns overall compliance; ensures there is an implemented Computing/Online Safety/Acceptable Use framework; line-manages the Computing Lead; and confirms that web filtering/monitoring are resourced, reviewed and embedded within safeguarding. **2) Safeguarding Ownership & Operational Oversight** • **Designated Safeguarding Lead (DSL) — James Savage (Deputy Headteacher)** Leads safeguarding integration of filtering/monitoring; understands how alerts and logs are generated; reviews concerns; triggers swift responses (CPOMS entries, parent contact, Early Help, police) and evaluates filtering/monitoring effectiveness with leadership and the technical partner. • **School Business Manager (SBM) – Nicola McGee** Shares operational oversight of filtering/monitoring with the DSL and Headteacher; ensures SLA controls, access

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			permissions, and data-protection expectations are in place; coordinates with MGL on change control and incident response. • **Computing Subject Leader – Olivia Farrington** Keeps abreast of technical and pedagogical developments; supports staff understanding of the filtered environment; liaises with the DSL/Headteacher on risks identified in lessons; and contributes to annual policy/filtering reviews with MGL. **3) Technical Provision & Change Control** • **Technical Partner — MGL (via SLA)** Provides and maintains the **professionally managed** web-filter and associated monitoring controls; keeps filter lists and categories **up-to-date**; supports incident triage; and participates in annual reviews and any mid-year reconfiguration required by safeguarding intelligence. • **Change Requests / Exceptions** Any request to open/relax categories, whitelist/blacklist sites, or modify monitoring thresholds follows an **approval route**: Computing Lead → SBM/DSL → Headteacher (final sign-off) → MGL implementation with audit trail. **4) Day-to-day Use & Human Monitoring** • **All Staff (Teaching & Support)** Model compliant use; supervise pupil activity;

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			respond to filtering blocks appropriately; report suspicious activity, repeated blocks, or concerning searches immediately to the DSL; and record safeguarding concerns on CPOMS. • **Class Teachers & TAs** Plan for safe, filtered access in lessons; use the AUP to reinforce boundaries; and inform the Computing Lead/DSL of any curriculum sites/apps that require review under change control. • **Pupils** Follow the AUP; report upsetting or blocked content appropriately; and understand that filtering exists to keep them safe and that attempts to bypass are breaches of policy/behaviour standards. • **Parents/Carers** Receive regular guidance (e.g., newsletters) and are expected to support age-appropriate app usage and home filtering/controls, reinforcing the school's messages. **5) Escalation Pathways (incidents & service issues)** **Online-safety incident (e.g., harmful search/attempted access):** Staff → **DSL** (same day) → CPOMS record → Parental contact / Early Help / Police as required → **MGL** consulted if filtering rules/blocks need tuning → **Headteacher/SBM** informed for governance and audit. **Service/performance issue (e.g., legitimate teaching**

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**site blocked or over-blocking):** Teacher → **Computing Lead** → **SBM/DSL** approval → **MGL** change request → **Headteacher** sign-off for category changes → Record outcome in the change log/annual review. **6) Review & Accountability Cycle** • **Annual**: Web-filter review and Computing Policy review (includes filtering/monitoring arrangements) with MGL and leadership. • **Termly**: DSL/Headteacher report to governors summarising filtering/monitoring themes, incidents, and curriculum/parent comms responses. • **Ongoing**: AUP training/refreshers; incident-led reconfiguration; curriculum whitelisting via change control.
Standard #2 - Review your filtering and monitoring provision at least annually – Where and how is your annual review carried out and documented (this section of this document is intended to be used as your review if you so wish)? – Who is present for this review, where are results logged and how are actions followed up on? – Is the provision safeguarding-driven, rather than based on convenience or 'how it always was'? – Is there sufficient technical input to be realistic and well informed, and sufficient safeguarding input that decisions are based on the best way to keep children safe and teach effectively?	🟩			Banks Road Primary meets the DfE requirement to **review filtering and monitoring systems at least annually** through a structured, policy-driven, safeguarding-led approach. Evidence from the ICT Acceptable Use Policy and the MGL Computing Policy shows that annual review is both mandated and embedded in operational practice. **1. Annual review cycle formally required and scheduled** The **MGL Computing Policy** explicitly states that: • *"Web filters are kept up-to-date,"*

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
– Has care been given not to be too restrictive and 'overblock' by impacting teaching and learning, by removing so much risk that pupils do not learn about the risk online they would face at home or sex education terms are blocked? – Are systems in place to identify if a review is needed more than annually (e.g. if there has been a significant change)? – How is your review informed by the latest trends nationally and in school? – How are outcomes of the review communicated with all staff? – How are 'regular checks' carried out, by whom and how often; where are these checks documents; how are the results fed back to the DSL and actions decided/followed up on? – Do checks cover these questions: ○ Are the key things still blocked/allowed as we need/think they are? ○ Are we overblocking in any way? Is filtering ACTIVE EVERYWHERE (all connections & devices & users)? ○ Is Safe Search ENFORCED (can't be turned off) EVERYWHERE (as above)? ○ Is the YouTube mode enforced as expected? ○ Are there concerns about students bypassing blocks? ○ Have we asked staff for feedback?	🟩			• filtering provision is reviewed **annually**, • and the entire Computing Policy (including filtering arrangements) is reviewed **annually as part of the school's policy review schedule*. This ensures that the filtering system is **not static**, and that leaders formally evaluate whether it continues to meet safeguarding requirements, technical standards and curriculum needs. **2. Leadership-led annual filtering review** Your ICT Acceptable Use Policy assigns direct filtering oversight and review responsibilities to: • **Headteacher** • **School Business Manager** • **DSL (Designated Safeguarding Lead)** • supported by **MGL technical specialists** This governance model ensures the annual review is: • **multi-disciplinary** (safeguarding + technical + operational) • **strategic** (led by senior leaders) • **documented** (policy review, AUP alignment, filtering logs, incident patterns) The DSL's role guarantees that the **safeguarding impact** of filtering is assessed annually—not only its technical performance. **3. Monitoring systems reviewed alongside filtering** The ICT AUP confirms the school must evaluate not just

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			filtering but the **monitoring** system used to detect concerning online activity, including: • internet activity logs • user alerts • attempts to access blocked content • email and network usage patterns This satisfies the DfE requirement that **monitoring** must also be reviewed annually to ensure it remains effective, proportionate and correctly configured. **4. Annual review is informed by live safeguarding intelligence** Filtering and monitoring reviews draw on: **CPOMS records** Patterns in online-safety incidents, attempts to bypass filters, or concerning digital behaviour are used to determine whether filtering categories need tightening or adjustments. **Online safety newsletters & emerging risks** The Computing Lead's parent newsletters reflect analysis of **current online risks** (e.g., group chat misuse, inappropriate language, impersonation), and these inform adjustments to filtering priorities. **Curriculum delivery data** Computing and PSHE staff identify whether legitimate educational sites were blocked or whether pupils require safer search configurations. This ensures the annual review is **evidence-based**, not administrative.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**5. SLA with MGL strengthens the review process** Your MGL Computing Policy confirms the school holds an active **Service Level Agreement (SLA)** with MGL, who: • maintain the filtering platform • update filter lists • support incident triage • advise on configuration changes • assist with annual review analysis This ensures the annual review is supported by **expert technical input**, meeting the DfE expectation that filtering must be *technically credible and professionally managed*. **6. Annual review impacts policies, curriculum and parental engagement** Outcomes of the review feed into: • updated AUP requirements • curriculum amendments (e.g., adjusting units like “Staying Safe Online” or “Social Media & Being Safe Online”) • parental communication (e.g., newsletters on new risks) • safeguarding documentation (DSL termly report, governor oversight) This shows annual review is **active and consequential**, influencing whole-school systems.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
Standard #3 - Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning – What does your system block/allow, for whom, where (eg home v school) and most importantly why? (NB you could either include this here or a link to an external document) – How is it flexible depending on context (e.g. what is allowed for older pupils only or with risk mitigations)? NB – the DfE standards state that a different staff and student policy is a minimum; best-practice is seen as much more granular. – Where do you deviate from the recommendations of your provider and/or other expert advisers, and WHY? What are the mitigations? – How does this support your current setting/cohort, their needs and recent safeguarding harms and trends? – What have you changed in the past year to improve the system? – What have you changed in the past year in response to safeguarding / behaviour / PHSE team input? – How are pupils taught to manage risk and allowed access to more content as they grow older? – What is your approach to generative AI sites (which can generate useful images/text/videos but also highly sexualised content, encourage self-harm or other inappropriate items)? – Are you only using gen AI websites that meet the Jan 25 DfE 'Generative AI: product safety expectations' and with regard to DfE document 'Generative artificial intelligence (AI) in education'? – Search engine/s: ○ Which do you allow and are all others blocked? ○ Do these allow safe search to be enforced?	🟩			Banks Road Primary's filtering provision successfully prevents access to harmful or inappropriate online material, while still enabling pupils and staff to access the resources needed for a broad, rich, and well-sequenced curriculum. The approach is balanced, safeguarding-led, and underpinned by clear policy expectations and technical controls. This section draws on evidence from the **ICT & Internet Acceptable Use Policy**, the **MGL Computing Policy**, and the **Computing curriculum documentation**. **1. Strong technical filtering that blocks harmful and inappropriate content** The **MGL Computing Policy** makes clear that the school provides a *safe online environment* through the use of **filtered internet access**, explicitly designed to prevent pupils from accessing inappropriate content. It states that: • *"Web filters are kept up-to-date in order to ensure that pupils don't access inappropriate materials."* • Filtering is recognised as essential to protecting children in a digital environment and sits alongside the Online Safety Policy to block harmful content. The **ICT Acceptable Use Policy** reinforces this by confirming that the school uses filtering that actively blocks: • harmful content • obscene or offensive material

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
○ Do these have embedded AI responses/if so how is this age appropriate? ○ Is the above covered in your regular checks schedule? – Which YouTube restricted mode do you use, why and how is it regularly checked? – Is effective RSHE possible insofar as pupils can access sex education and safely search for correct anatomical words? – Does your provider block the relevant illegal content lists (check their submission to UK SIC)? These are CTIRU, IWF, PIPCU. – Do teachers regularly confirm that teaching and learning is not impacted by overblocking, and the risk balance is correct and pupils confirm that they are learning about managing risk online in lessons and ad hoc opportunities? – Do students confirm that using devices at school helps them manage this on private devices at home? – Are staff, pupils and parents reminded that the internet can never be 100% safe and things will go wrong but as a school we will learn from it and improve, always provide a much safer environment than at home and empower school staff to use times when things go wrong as teachable moments?	🟩			• radicalised, extremist or violent content • pornographic or age-inappropriate sites • illegal content or malicious domains This demonstrates the school meets the DfE requirement that filtering must provide a **high level of protection** against known categories of harm. **2. Filtering aligned with primary-age appropriateness** The filtering system is configured with **age-appropriate restrictions**, ensuring that: • children only access content suitable for KS1 and KS2 • blocked categories reflect primary safeguarding needs (e.g., gaming chat platforms, unmoderated social media, adult content) • pupils understand why filtering exists and how it keeps them safe, supported through RSHE, PSHE and Computing teaching Online safety units such as **Y2 "Staying Safe Online"** and **Y6 "Social Media & Being Safe Online"** rely on a filtered environment to model safe behaviour without risk of exposure. This aligns directly with the DfE expectation that filtering should be **specifically tailored to the age range of the school**. **3. Filtering does not "over-block" or hinder teaching and learning** Banks Road's approach ensures filtering supports

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			effective learning rather than restricting it. This balance is achieved through: **a) Controlled whitelisting and change-control** Requests to unblock curriculum content follow an approval pathway (Teacher → Computing Lead → DSL/SBM → Headteacher → MGL). This prevents accidental access to harmful content while allowing curriculum-essential sites to be authorised. **b) Curriculum access remains broad** Teachers use a wide range of online tools (e.g., coding platforms, digital research tools, CEOP resources, online publishing tools, cloud platforms), all accessible within the school's filtered environment, demonstrating that filtering does **not unreasonably restrict**: • Computing curriculum delivery • digital literacy lessons • password practice, email safety, and safe searching sessions • creative digital work (podcasting, animation, publishing) **c) Teachers plan confidently within filtered systems** The MGL Computing Policy confirms that teachers are supported by the Computing Lead and technical partner to ensure digital tools are accessible and functional, and that filtering is configured to enable safe use of iPads, laptops, and coding hardware such as **Micro:Bits, BeeBots and Spheroes**. This avoids the "over-blocking" that the DfE warns can undermine the curriculum.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**4. Filtering supports safe exploration and risk-education** Rather than simply blocking, filtering is used to: • enable pupils to learn *how* search engines work (Y4 "Smarter Searching") • support critical evaluation of online content (Y3+ curriculum) • provide safe environments to explore email, messaging, and internet services • reinforce safe reporting routes when something is blocked or concerning Because filtering is configured appropriately, pupils experience **realistic but safe** digital conditions. This supports the DfE requirement that filtering must not "overly restrict" learning in a way that prevents pupils from gaining digital resilience. **5. Filtering reinforced by behaviour and device policies** The Mobile Phone Policy enforces a strict *"no use, no sight, no sound"* rule for pupils' personal devices on site, which prevents: • unfiltered 4G/5G data access • unmonitored apps and social media • bypassing the school's filtering system This ensures the filter applies consistently and avoids the common DfE-identified risk that pupils bypass restrictions using personal devices.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**6. Safeguarding-first approach ensures filtering remains proportionate** The DSL, SBM and Headteacher **jointly evaluate** the balance between safeguarding and curriculum needs, ensuring: • filtering blocks harmful content **effectively** • teaching and learning are **not inhibited** • requests for site access always undergo safeguarding consideration first This reflects the DfE requirement that filtering must be both **protective and proportionate**.
Standard #4 - Have effective monitoring strategies that meet the safeguarding needs of your school or college ***NB - This standard is mainly about monitoring, not filtering. Please ensure you are aware of the difference (see intro to DfE Standards); but when it comes to checking reports/logs for your filtering, you may wish to consider these points:*** – Which regular reports are run and on what? What is the purpose of these checks, what is looked for? – Who checks logs and how does this happen when there is an incident that needs investigating? – Can you report on what students search for (NB this requires decryption)? – How has your system been changed over the past year to make it safer or more appropriate in other ways?	🟩			Banks Road Primary operates **layered, proportionate monitoring** that combines **technical monitoring** (system logs/alerts) with **human monitoring** (staff supervision, curriculum-embedded observation, DSL oversight). Monitoring is explicitly tied into safeguarding routes (DSL triage, CPOMS recording, parental contact, external agency referrals), so concerns move from detection → response → review. Roles and escalation are named in policy, and monitoring is reviewed at least annually alongside filtering. **1) Governance, Roles & Accountability** • **Named oversight**: The **Headteacher**, **DSL**, and **School Business Manager** hold responsibility for understanding and overseeing the school's monitoring systems and processes, supported by **MGL** as the technical partner. This ensures monitoring is part of safeguarding—not just "IT". • **Computing Subject Leader**: Keeps staff

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
– Do logs and reports from your system enable you to identify users – where this is not possible, what risk mitigations do you have in place (e.g. stricter filtering if you cannot tell the user) or manual ways of logging users (e.g. if a set of ipads cannot be tracked to a user, note on paper who was issued each device)? – How does what you do here tie in with any technical monitoring system you may have (given that most of Standard 4 relates to dedicated monitoring systems)?	🟩			informed about emerging risks observed via monitoring patterns and classroom practice; liaises with the DSL where themes (e.g., language in group chats) indicate a need for whole-school action or parent communication. • **Annual review**: Monitoring effectiveness is reviewed **at least annually** (with MGL input) as part of the computing/online safety policy cycle. **2) Technical Monitoring – What we capture and how we act** **Scope** (examples; precise capabilities are managed via SLA and AUP): • **Web activity/attempts**: Inspection of internet activity and **attempted access to blocked content** (e.g., repeated searches for harmful terms) triggers DSL review and teaching or pastoral follow-up. • **User/device context**: Monitoring is aligned with **school-managed devices/platforms** (e.g., iPads/laptops; Office 365/approved services) to surface concerning patterns while keeping oversight proportionate. • **Change-driven tuning**: Where monitoring shows legitimate curriculum needs are being impeded—or where risk profiles change—the Computing Lead/DSL/SBM submit a **controlled change request** to MGL to tune categories/alerts, with Headteacher sign-off and audit trail. • **Data protection & proportionality**: Monitoring is

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			used **only for safeguarding/operational purposes**, with access limited to authorised staff, and with records handled under the school's data-protection expectations in the AUP. **Response workflow** 1. **Alert/pattern detected** (e.g., concerning search term, repeated block attempts). 2. **Staff → DSL same day**; record on **CPOMS** with chronology, evidence (screenshots/URLs where appropriate) and initial action. 3. **DSL triage**: assess risk; contact parents; apply early help; liaise with external services/police where required; evaluate whether configuration/training needs updating. 4. **Review**: incorporate learning into newsletters (parents), curriculum (PSHE/Computing), and staff briefings. **3) Human Monitoring – In-class supervision & curriculum-embedded practice** • **Active in-lesson supervision**: Staff supervise device use; apply immediate, **live formative checks** (questioning, visualiser modelling) to spot misconceptions or unsafe choices "in the moment", then adapt the lesson. • **Structured pupil responses**: Where unsafe choices are identified in work, pupils use **purple-pen** responses to correct and explain safer alternatives, closing the loop and

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			evidencing changed behaviour. • **Curriculum-triggered monitoring points**: Units such as **Y2 “Staying Safe Online”** and **Y6 “Social Media & Being Safe Online”** include scenario tasks that allow staff to monitor decision-making and vocabulary (privacy, reporting, PEGI, scams), and quickly escalate concerns. • **Pastoral observation**: Staff note patterns (e.g., online fallouts spilling into school), inform the DSL, and reinforce expectations via assemblies/PSHE. **4) Monitoring beyond the filter (BYOD & out-of-school issues)** • **Personal devices**: The **Mobile Phone Policy** enforces *“no use, no sight, no sound”* on site, reducing unfiltered data risks. Any concern reported (e.g., an out-of-hours group chat incident) is treated as a **safeguarding matter**, recorded on CPOMS, and addressed via parents/DSL even if it occurred off-site. • **Parent partnership**: Regular **Online Safety Newsletters** guide families on reviewing chat groups, privacy settings and respectful language, so monitoring continues at home in partnership with school. **5) Evidence-informed improvement cycle** Monitoring isn’t just detection—it **drives improvement**:

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• **CPOMS pattern analysis** (termly) informs DSL reports to leaders/governors and shapes subsequent curriculum tweaks and parent comms. • **Newsletters & staff briefings** reflect live trends (e.g., impersonation in group chats), building community awareness and prevention. • **Annual review with MGL** ensures monitoring thresholds and alerting remain **age-appropriate, proportionate and effective**. **6) Staff Competence & Confidence** • **Policy-driven expectations**: Staff know how to **report** online concerns, what constitutes a **monitoring signal**, and when to escalate to the DSL/Headteacher (low-level concerns and above). • **Ongoing updates**: The Computing Lead and DSL use parent communications and staff notices to keep colleagues **alert to new risks**, reinforcing professional vigilance in monitoring. **7) What we check in monitoring reports/logs (practical pointers)** When reviewing monitoring data (including filter logs when relevant), leaders/staff consider: • **Repeated block attempts** for specific terms/sites (signal of intent/risk). • **Time-of-day clustering** (e.g., break/lunchtime

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			patterns) suggesting supervision/education adjustments. • **Cohort trends** (e.g., upper KS2 queries about social media), informing newsletters and curriculum emphasis. • **False positives/over-blocking** that impede lessons—actioned via the change-control route to MGL.
Filtering training – Has your technical team attended training on your filtering platform/s to understand exactly how it works, how it is set up and what the options are in order to inform a strategic filtering approach and implement DSL/SLT requirements? – Has your safeguarding team also attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what filtering can/should do to inform the approach? – Are both technical and safeguarding colleagues taught that when content is blocked but required for access, it is best practice to allow the site rather than the entire category? – Is there an awareness of the wide-range of content in categories such as shopping (even the most popular shopping site sells sex toys) and entertainment (which would include the latest from Strictly but also explicit discussion of sex and other adult themes in the same way these might come up on television)? – Have you included F&M in your start of year safeguarding briefing and/or other insets to ensure all staff are aware of the importance of this area, that the DSL team drive strategy, and that they are the eyes and ears to pass on gaps or overblocking?	🟩			Banks Road Primary delivers **structured, comprehensive and recurring training** on filtering, monitoring and digital-safeguarding expectations. This ensures all staff understand how the filtering system protects pupils, how to act on alerts or blocked-content attempts, and how filtering sits within the wider safeguarding framework (KCSIE, AUP, DSL reporting, CPOMS). Filtering training is delivered through a **multi-layered programme** involving MGL (technical partner), the DSL, School Improvement Liverpool and national online-safety experts. As a result, staff knowledge is consistently refreshed, up-to-date and practically grounded. **1. Whole-staff filtering & monitoring training (statutory + technical)** **MGL-led whole-staff training (15/04/24) – Filtering & Monitoring** All teaching staff received direct training from MGL on: • KCSIE updates relating to filtering and monitoring • what constitutes a filtering or monitoring incident

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• how to recognise and respond to cyber incidents • what to do immediately if a concerning digital event occurs • how the school's filtered environment interacts with safeguarding pathways This provides strong alignment with DfE Filtering & Monitoring Standards, which require staff to understand both filtering limitations and the school's escalation model. **2. Whole-staff cyber-security training strengthens filtering understanding** **Cyber Security Training – whole staff (29/09/25)** Delivered by MGL, this session explicitly covered: • the school's cyber-security policies • safe use of digital systems and AI • recognising data-breach indicators • keeping themselves and the school safe online This training helps staff understand *why* filtering is configured in certain ways and how it links to wider threat protection and data-protection requirements. **3. SLT-specific training deepens leadership oversight of filtering** **Smoothwall Safeguard Executive Training (05/10/23)** The DSL received high-level industry-standard training on: • filtering & monitoring best practice

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• current digital-risk landscape • updates in KCSIE • threshold understanding for alerts This strengthens SLT capacity to lead filtering decisions, review logs, interpret patterns and respond appropriately. **DSL refresher training (annual)** Your training log shows DSL and deputy DSL training annually (e.g., 23/09/24; 22/09/25; previous years). These courses include updates on safeguarding technology expectations and threshold decisions. This ensures filtering oversight is **current, informed and compliant**. **4. Filtering positioned as part of the whole-school safeguarding system** Banks Road's AUP requires: • the **Headteacher**, **DSL**, **SBM** and **MGL** to jointly oversee filtering and monitoring systems • staff to report concerns to the DSL immediately Your training reinforces this consistently: • staff safeguarding training includes online concerns and filtering-linked reporting (e.g., annual safeguarding sessions: 13/10/25; 07/10/24; 27/10/23) • online-safety sessions consistently emphasise recognising block attempts, suspicious searches and unsafe patterns • Prevent training (multiple years) helps staff

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			understand how filtering interacts with radicalisation risks and extremist content online This ensures filtering knowledge sits within a **broader safeguarding mindset**, not isolated technical awareness. **5. Training supports rapid, correct escalation of filtering incidents** Filtering issues—e.g., repeated blocks, concerning search terms, access attempts—are treated as **safeguarding incidents**, not IT issues. Training log evidence shows repeated CPD that ensures staff know: • what to do *in the moment* (Online Safety: The Essentials – 11/11/25) • how to escalate concerns immediately to DSL • how to record incidents on **CPOMS** (included in all annual safeguarding training) • how to interpret blocked content as *potential signals of harm* This meets the DfE requirement that “staff understand the filtering system and know how to act on concerns.” **6. Pupils receive filtering-aware online-safety teaching** Filtering does not stand alone; it is reinforced through pupil-facing sessions: • Online Safety Day workshops (multiple years) • Digital Community Police Officer sessions

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			addressing blocked-content reasoning, safe searches, digital footprints (Years 3–6) • Online Safety workshops in KS2 (e.g., 05/03/20; 08/05/24) These reinforce why filtering exists and what to do when pupils encounter digital concerns—essential for DfE “education + systems” expectations. **7. AI training integrated into filtering understanding** Your AI Policy includes: • expectations around data security • preventing entry of pupil data into external systems • mandatory evaluation of new tools • spot checks of AI-generated content Staff are trained in safe AI use (included in cyber-security training 29/09/25), helping them understand how filtering interacts with: • AI-related risks • deepfakes and impersonation • unsafe prompts • potential bypass attempts This places Banks Road ahead of national expectations.
Rationale / team effort – Do your technical and safeguarding teams meet to discuss your filtering needs and document your approach regarding what is allowed / not in school and the safeguarding-driven rationale? – Is this up to date, reflected accurately (and updated) in policies and	🟩			Banks Road Primary’s training model is built on the belief that **keeping children safe online is everyone’s responsibility**, and that effective online-safety and cyber-security education requires a **whole-school, multi-agency and multi-disciplinary effort**. The

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
practice, including how your approach and settings do not 'over-block', and shared with parents, staff and governors and ready to show to Ofsted?	🟩			rationale underpinning your training approach is clear across your policies and training records: **Staff, DSLs, Governors, Pupils, External Partners and Technical Experts all contribute to an integrated safeguarding culture.** This section explains how that team effort works in practice. **1. A safeguarding-first rationale** The training log shows a culture where safeguarding—and specifically online safety—is treated as a **core professional responsibility**, not an add-on. This is evident in the school's: • **annual whole-staff safeguarding training** (13/10/25; 07/10/24; 27/10/23) ensuring all staff know signs, indicators, digital risks, and CPOMS processes. • repeated training in **PREVENT**, **child exploitation**, **bullying**, **online abuse**, and **digital risk**, across multiple years. • integration of filtering/monitoring into safeguarding training (15/04/24, MGL session). This demonstrates a shared rationale: **online safety = safeguarding = everyone's job.** **2. Shared ownership across the school team** **DSL & Deputy DSL** DSLs lead safeguarding training and ensure online safety is embedded in procedures. They receive **annual**

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**refresher training** (e.g., 22/09/25; 23/09/24; 19/09/23) to keep their expertise fully current. **All staff** Teachers, TAs, office staff and trainees attend: • cyber-security training (29/09/25) • online safety essentials (11/11/25) • filtering and monitoring training (15/04/24) This ensures all adults—across all roles—understand their duties. **Governors** Governors receive **Safeguarding for Governance training** (03/2025), building their capacity for strategic oversight and compliance monitoring. Under the AI Policy, the **IT Governor** also plays a formal role in approving or challenging AI tool adoption. **Pupils** Pupils themselves form part of the safety ecosystem through: • Digital Community Police Officer sessions (Years 3–6) • Online Safety Days (multiple years) • Workshops on cyberbullying, grooming, digital footprints and safe search behaviour Children are equipped with knowledge, vocabulary and help-seeking strategies, forming an important layer of risk identification. **3. Multi-agency partnership strengthens training**

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**impact** Banks Road's training record shows extensive collaboration with external experts: • **MGL** – technical, cyber-security, and filtering/monitoring training (29/09/25 and 15/04/24) • **Smoothwall / national online safety experts** – leadership briefings (05/10/23) • **Liverpool PREVENT team** – regular Prevent training (15/09/25; 10–11/03/25; 27/10/23) • **School Improvement Liverpool** – DSL training, safeguarding briefings, e-safety workshops (various years) • **Police & Fire Services** – digital risk, cyber-safety, hate crime, anti-social behaviour (multiple years) • **Anti-bullying charities** – cyberbullying and peer support (multiple years) This external input enhances credibility, accuracy, and up-to-date knowledge, ensuring staff understand the *real* risks children face. **4. Training aligns with and reinforces school policy** Across the AUP, AI Policy, and RSHE curriculum: • Staff are *expected* to understand filtering, monitoring, safe AI use, safe communication boundaries and reporting routes. • Training ensures those expectations are not theoretical—they are lived practice. • AI training (MGL, 29/09/25) aligns with the AI

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			Policy’s requirements for transparency, data protection, and ethical use. This creates a virtuous cycle of policy ↔ training ↔ implementation. **5. Training is continuous, documented and cumulative** The training log shows: • Consistent safeguarding CPD from 2017 to 2026 • Regular online-safety and cyber-security training • Governor CPD • Pupil workshops every year • External speakers annually This cumulative model ensures: • no staff group is left behind • new threats are incorporated quickly • cultural expectations are reinforced over time The result is a **shared organisational memory** of best practice. **6. Team effort: communication & escalation** Banks Road’s CPOMS-based safeguarding system depends on: • staff recognising early signs (training gives them this) • DSLs responding rapidly (enabled by DSL training cycles) • leadership reviewing patterns (from documented CPOMS logs)

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• MGL supporting technical analysis where needed Training strengthens this shared responsibility. **Summary: A whole-community safety culture** Banks Road's training rationale is built on: • **shared responsibility** • **multi-agency expertise** • **strong leadership oversight** • **policy-aligned content** • **consistent documentation & reinforcement** It is one of the strongest areas of your online-safety ecosystem.
BYOD – If you allow 'bring your own device', what measures are applied to these devices to ensure the school internet cannot be used inappropriately simply by switching to a BYOD? network	🟩			Banks Road Primary adopts a **restrictive, safeguarding-led posture** toward BYOD. Pupils are **not permitted** to use personal devices on site; staff and visitors may use personal devices only under **strict, role-based conditions** and **never** for processing pupil personal data, unless explicitly authorised and compliant with school data-protection controls. This approach prevents unfiltered access, reduces attack surface, and keeps safeguarding oversight within school-managed systems. **1) Pupils (no BYOD)** • **"No use, no sight, no sound"** applies to all pupil mobile phones and smart devices at all times on the school site (including transitions, breaks, and clubs). Where a phone is brought for travel safety or exceptional needs, it is **handed in and stored**

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	- Evidence/details (e.g. documents, training, reminders) & dates
	🟩			securely; pupils cannot access it during the day. - Personal hotspots and mobile data are implicitly prohibited by the above; attempts to use personal devices or to bypass the school network constitute a **behaviour breach**, triggering staged consequences as per the Behaviour Policy. **Safeguarding impact:** enforcing no-BYOD for pupils prevents unmonitored 4G/5G access and ensures learners remain within the school's filtered/monitored environment. **2) Staff personal devices** - Staff may carry personal phones, but **must not** process pupil personal data or confidential school information on them (including through AI tools) and **must not** use personal devices for photography/video of pupils. Any *operationally necessary* use (e.g., MFA prompts) occurs **out of sight of pupils** and under the Code of Conduct. - Remote access is via **approved, secure cloud platforms only** on **school-owned devices**; private equipment must **not** be used to store or process personal data without explicit authorisation and encryption controls. - Where a limited exception is authorised (e.g., a specific role requirement), it must be **formally approved** by the Headteacher/SBM, with technical safeguards (encryption, auto-lock, no local storage) and revocable at any time. **Safeguarding & data protection:** staff device use is

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			bounded by the AUP's **data-minimisation** and **access-control** rules; breaches follow the Disciplinary Policy and data-breach procedures. **3) Visitors, volunteers, and contractors** • Visitors/volunteers **must not** use personal devices where pupils are present and **must not** capture images of pupils. Device use is restricted to private areas (e.g., staffroom/reception), and only for non-school purposes unless explicitly authorised. • **Wi-Fi access** for visitors is **not granted by default**; the Headteacher may authorise temporary access **only** where necessary to fulfil the visit purpose. Staff must **never** share Wi-Fi credentials without authorisation. **4) Network access & segmentation** • BYOD does **not** connect to teaching/admin networks. The AUP makes clear that connecting any device to the school network requires **authorised approval**; only school-managed devices use the filtered/monitored VLANs that support curriculum and safeguarding oversight. • The MGL policy confirms an SLA-based model in which the computing lead and technical partner maintain approved inventories, ensure **filters are kept up-to-date**, and manage change-control for any access exceptions; obsolete/broken devices are handled in line with data-protection

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			requirements. **5) Risk scenarios & controls** • **Hot-spotting / tethering:** treated as an attempt to bypass safeguarding systems; managed as a behaviour/staff-disciplinary issue as applicable. Record on CPOMS where safeguarding is implicated. • **Image capture / messaging apps:** strictly prohibited for staff and visitors; any incident is escalated to the **DSL the same day** and handled under Safeguarding and Managing Allegations procedures where relevant. • **Data handling on personal devices:** prohibited unless explicitly authorised (see §2). Any suspected breach follows the data-breach procedure and may trigger disciplinary action and external reporting. **6) Change-control & approvals** Any request that would alter the BYOD posture (e.g., to enable a particular visitor device for a demonstration) follows the **approval route**: Requestor → Computing Lead → **SBM/DSL** risk check → **Headteacher** sign-off → **MGL** implementation (time-bound, auditable, least-privilege). **7) Communication & reinforcement** • Expectations are posted at reception and reiterated in visitor briefings; staff are reminded via the AUP and Mobile Phone Policy; parents are

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			informed that pupil devices are not for use in school and that **group-chat issues out of school** should be reported to the DSL for support.
Devices at home – Have you applied filtering to school devices when sent home with students? – Given that schools cannot protect parent/child devices, do you remind parents about how to set controls on their home internet/phones/devices etc?	🟩			Banks Road Primary recognises that most online risk and digital decision-making now occurs **at home, on personal devices**. Our approach is to **educate, equip and partner** with families so that expectations are consistent between school and home, and pupils use technology safely and respectfully wherever they are. This section draws on the **ICT & Internet Acceptable Use Policy (AUP)**, the **Mobile Phone & Smart Devices Policy**, the **MGL Computing Policy**, and the **Online Safety Newsletter** content shared via ClassDojo. **1) What we ask of families** **Age-appropriate platforms and supervision** We ask parents to ensure children only use apps and platforms that are age-appropriate, to keep accounts private, and to supervise use—particularly for **group chats**, where unkind/inappropriate language and impersonation can arise. (Our newsletters explicitly remind families that many messaging apps are **13+** and offer practical steps to review chats and privacy settings.) **Respectful language and behaviour online** We reinforce that words online have the **same impact** as words said face-to-face; families are encouraged to set clear rules for language and kindness at home, with examples in the newsletter and in RSHE/PSHE lessons. **Report concerns early** Parents are encouraged to contact school promptly if

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			online issues spill into school relationships or wellbeing. Staff will log safeguarding-relevant concerns on **CPOMS** and the DSL will triage and support next steps (including signposting and liaison with external agencies if needed). (Reporting expectations and safeguarding integration are set out in the AUP and whole-school assessment/recording processes.) **2) How school supports safe home use** **Regular parent communication (ClassDojo newsletters)** The Computing Lead shares **regular Online Safety Newsletters** that give families practical, “do-this-now” steps—e.g., checking privacy settings, reviewing membership of group chats, deciding when to leave a risky chat, and modelling respectful digital behaviour. These updates are responsive to **current trends** (e.g., inappropriate language in chats, impersonation), so advice remains timely and relevant. **Curriculum alignment** Computing (e.g., Y2 *Staying Safe Online*, Y6 *Social Media & Being Safe Online*) and RSHE teach pupils how to protect privacy, evaluate contacts/content, understand image-sharing risks, and **know how and where to report** concerns. This equips pupils to carry strategies from school **into home settings**. **Clear boundaries for devices brought to school** Our “**no use, no sight, no sound**” rule for pupil devices prevents unfiltered 4G/5G use on site, and ensures any device that must be brought for travel safety is **handed in and stored**. This separation reduces the chance that

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			out-of-school issues escalate during the school day and clarifies accountability between **home-managed devices** and the **school-managed environment**. **Consistent safeguarding language** The AUP and newsletters use consistent, accessible wording so that parental expectations mirror staff guidance (e.g., “keep accounts private”, “review who can message/add your child”, “speak to us early”). **3) Practical guidance we promote for home** • **Know the apps**: Check age ratings; avoid under-age sign-ups; talk to children about why limits exist. • **Controls & privacy**: Turn on platform-level parental controls/filters; set accounts to private; limit who can add/message your child. • **Be involved**: Ask to **see the group chats** your child is in; agree family rules for language and posting; rehearse what to do if things go wrong (block/report/leave). • **Model good behaviour**: Adults model respectful language and sensible screen-time habits; children learn more from what we **do** than what we say. • **When to leave**: If a chat is unmoderated, includes impersonation or persistent nastiness, **leaving** is often the safest option—talk this through together so children understand the reasons. • **Tell school early**: If an online issue is affecting

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			learning, attendance or wellbeing, let school/DSL know; we will support proportionately and confidentially. (AUP sets the reporting routes and oversight.) **4) Data protection and safe handling at home** We ask parents **not** to share or post images/videos of other pupils without consent, and to discourage children from re-sharing other people's images. Staff never use personal devices to process pupil data or images; parents are encouraged to adopt the same caution at home (e.g., avoid posting class photos to personal socials). (Restrictions and rationale are set out in the AUP and Code of Conduct.) **5) How we escalate and follow up when home issues affect school** • **Record**: Staff log safeguarding-relevant incidents on **CPOMS** with evidence (screenshots/URLs) where appropriate. • **Triage & support**: DSL contacts parents, assesses risk, and agrees actions—this might include classroom strategies, pastoral input, or external referrals if thresholds are met. • **Educate**: We integrate learning back into lessons/assemblies and parent updates so the wider community benefits (e.g., newsletter items about risky group-chat dynamics and language). **6) Why this matters**

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			The **school-home interface** is where many online issues begin. By combining **clear school policies** (AUP, Mobile Phone) with **parent education** (newsletters) and **curriculum** (Computing/RSHE), we create consistent boundaries and shared language so that pupils can transfer safe choices **from school to home** and vice-versa.
Linked to the curriculum and safeguarding landscape – Is your filtering set up and updated to reflect the online-safety messages you teach and safeguarding concerns/cases in school? – Conversely, is learning from filtering findings used to inform the curriculum?	🟩			Banks Road Primary's filtering, monitoring and wider digital-safeguarding systems are **explicitly intertwined** with its curriculum design and safeguarding culture. The school does not treat online safety as a technical requirement; instead, it is taught, reinforced and applied through a **joined-up model** where curriculum knowledge, pastoral responses and protective systems work together to keep pupils safe. **1. Filtering and monitoring are mapped directly onto curriculum coverage** **Computing Curriculum (EYFS–Y6)** The Computing long-term plan contains **explicit online-safety teaching in every phase**: • **Nursery/EYFS** – recognising who can be trusted and understanding safe use with adults. • **KS1** – personal information, passwords, trusted adults, "Staying Safe Online" (Y2). • **Lower KS2** – email safety, clickbait, image editing & consent, evaluating reliability of information. • **Upper KS2** – social media safety, PEGI ratings, respectful communication, in-app purchases, safe online publishing.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			Filtering and monitoring support this by: • providing a **safe environment** for searching, email practice and content creation • blocking unsafe external content so children can practise skills without exposure • enabling teachers to identify patterns of access or attempted access that reveal curriculum gaps • supporting scaffolded discussions around blocked content, risk and digital boundaries This demonstrates strong alignment between **curriculum intent and digital infrastructure**. **2. RSHE curriculum establishes the safeguarding frame for online behaviours** The 2026 RSHE Draft Policy states that pupils must be taught: • respectful online behaviour, privacy and boundaries • risks linked to image-sharing, permanence of content and deepfake manipulation • how to recognise unsafe contact and report concerns • evaluating online information and understanding age restrictions (including 13+ platforms) Filtering and monitoring reinforce this by: • preventing access to age-inappropriate platforms in school • surfacing harmful search patterns that indicate

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			safeguarding risk • prompting DSL follow-up and curriculum re-emphasis • supporting safe exploration of curriculum content (e.g., “Being Safe Online”) This creates a loop where **curriculum teaches protective behaviours**, and **monitoring verifies understanding**. **3. PSHE provides the relational, emotional and ethical context** The PSHE long-term plan (2026) contains online-safety-related themes such as: • friendship conflict online (Y3) • positive/negative online friendships (Y3) • kindness, inclusion, identity and discrimination (across all years) • scams, online fraud, gaming payment models (Y5–6) • image-sharing, coercion and peer pressure (“Send me a selfie”, Y6) Filtering/monitoring link to this by identifying: • unkind or unsafe digital behaviours spilling into school • patterns (e.g., repeated attempts to access certain terms) indicating gaps in understanding • specific cohorts needing targeted PSHE or pastoral input

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• safeguarding concerns requiring CPOMS recording and DSL intervention Thus, PSHE provides the **context and language** pupils need to understand and respond to monitored risks. **4. Filtering and monitoring reinforce whole-school safeguarding expectations** Across policies, the school emphasises: • **safeguarding-first digital practice**, with DSL oversight of monitoring and response • **clear reporting routes** for concerns (staff, pupils, parents) • **structured follow-up** when patterns arise • **integration with CPOMS** as the central safeguarding record Filtering is therefore not simply technical protection but part of a **coherent safeguarding ecosystem** that includes: • behaviour policies for online misconduct • anti-bullying frameworks (including cyberbullying) • mobile device restrictions preventing unfiltered access • parent education and involvement **5. Annual review ensures alignment remains dynamic and current** The MGL Computing Policy requires **annual review of**

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**web filters** and **annual revision** of the Computing policy itself. This aligns filtering with: • updates to RSHE statutory guidance • emerging safeguarding risks identified through CPOMS • PSHE/Computing curricular updates • monitoring patterns (e.g., group chat issues) that inform parent newsletters The result is a **dynamic system**, continually informed by curriculum delivery and safeguarding realities. **6. Monitoring insights inform curriculum adaptation** Monitoring (technical + human) feeds directly into: • targeted reteaching where misconceptions appear (e.g., misuse of language online, misunderstanding privacy) • focused PSHE assemblies responding to real incidents • parent newsletters addressing real-time risk behaviours (e.g., impersonation) • curriculum sequencing adjustments when patterns occur across year groups • pastoral or group work where safeguarding concerns arise This creates a **feedback loop** where risks seen in monitoring shape curriculum emphasis, and curriculum knowledge reduces risky behaviours caught by monitoring.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**7. Strong school–home consistency completes the safeguarding landscape** Filtering/monitoring inside school are reinforced outside school by: • parental newsletters on group chats, language and age restrictions • RSHE curriculum teaching pupils what to do when at home • expectations shared at "Meet the Teacher" events • the school's BYOD stance preventing unfiltered devices on site This gives pupils **consistent boundaries** wherever they use devices.
MONITORING				
DfE Standard 4 and Monitoring Approach – Are you satisfied that overall your school is complying with standard #4 "You should have effective monitoring strategies that meet the safeguarding needs of your school or college"? – What are the key action areas for the school to improve on and improve compliance over the next 12 months? – How are all staff helped to understand the difference between filtering and monitoring? Do they understand these two sections (verbatim from DfE Standards): ○ "Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity [...] solutions do not block users from seeing or doing anything."	🟩			Banks Road Primary uses a **dual-layered approach** to monitoring: **Technical Monitoring (digital signals)** + **Human Monitoring (behavioural, curricular, pastoral)** Together forming an integrated safeguarding system. **1. Leadership-led oversight of monitoring** The AUP assigns explicit monitoring responsibility to: • **Headteacher** (overall DSL line-management and compliance ownership) • **DSL (Deputy Headteacher)** – primary lead for

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
– Are monitoring captures dealt with by the safeguarding team (not technical staff)? Who does what? – How does the safeguarding team find the time to deal with captures (do you have a human monitoring service that also looks at captures / are others supporting the team – if so are they safeguarding trained and aware of current trends)? – Is your approach to monitoring based on a strategic and safeguarding-driven rationale that has been made in discussion between safeguarding and technical teams? – Which of the four monitoring strategies listed in the DfE standards do you use, where and why? • Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. • Technical monitoring solutions rely on software applied to a device that views a user's activity. • Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. – Are all senior leaders, governors and staff aware of this rationale and which approaches are used where? – How is the system updated in line with the latest concerns around issues or users, new flags or keywords etc added? – Beyond the captures flagged immediately or daily, who uses the system to look for trends and compare with other systems? What is the methodology for this? – How are results from monitoring fed into the safeguarding reporting systems (e.g. CPOMS/myConcern) to ensure the 'safeguarding jigsaw' is not fragmented?	🟩			monitoring review, incident triage and safeguarding actions • **School Business Manager** – operational oversight, data-protection compliance, technical administration • **MGL (technical partner)** – supports technical configuration, alerting, and annual review This ensures monitoring is **actively supervised** by senior leaders and firmly embedded within safeguarding governance. **2. Technical monitoring: what, how and why** Banks Road uses professionally supported systems to monitor: • **Internet activity logs** – identifying concerning search terms, attempts to access blocked content, repeated high-risk queries • **Network-level device behaviour** – attempts to bypass filters or use unapproved services • **User-based patterns** – frequency and persistence of attempts, time-of-day patterns These signals trigger the DSL's involvement and CPOMS reporting, in line with safeguarding procedures. The technical monitoring system is **annually reviewed** through the Computing Policy's mandated cycle. **Response cycle** 1. Alert/flag identified 2. Staff → DSL immediately 3. DSL logs to **CPOMS** and evaluates risk

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			4. Parental contact / Early Help / external agencies if necessary 5. Curriculum adjustments or assemblies if patterns emerge This ensures every monitored concern feeds into a **safeguarding-first response**. **3. Human monitoring: real-time, teaching-embedded supervision** Because primary pupils often access devices during lessons, staff are a critical layer of monitoring. The school's approach includes: **Live supervision** • Staff circulate, observe screens and intervene immediately • "Live marking" and in-the-moment feedback as set out in the Assessment Handbook **Curriculum-embedded tasks** Lessons can reveal risk behaviours or misconceptions about: • privacy • online friends • content reliability • group chat behaviour • image-sharing decisions Examples include Y2 "Staying Safe Online," Y4 "Smarter Searching," and Y6 "Social Media & Being Safe Online."

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**Pastoral monitoring** Staff detect early signs of digital issues spilling into school (e.g., fallouts from group chats), report to DSL and address via PSHE. This human layer ensures that monitoring does not rely **solely** on logs—meeting the DfE expectation for proportionate, blended approaches. **4. Monitoring linked to safeguarding landscapes** Monitoring indicators feed directly into: **Safeguarding** • All concerning digital behaviour is logged in **CPOMS** • Patterns trigger DSL analysis and actions • Cross-reference with attendance, behaviour, SEND and pastoral profiles **Curriculum adaptation** If monitoring shows: • inappropriate language online • risky platform use • group chat coercion • repeated attempts to access mature content —these become topics for reteaching in PSHE, Computing or RSHE. **Parent communication** Online Safety Newsletters respond to **real threats**, e.g.: • impersonation • group chat bullying

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• inappropriate language Monitoring therefore drives **preventative education** and **community awareness**. **5. BYOD safeguards strengthen monitoring** The **Mobile Phone Policy** removes the risk of unmonitored, unfiltered access on personal devices: • *“No use, no sight, no sound”* prevents pupil BYOD bypassing monitoring • Personal devices cannot access the school network This ensures monitoring coverage is not weakened by personal 4G/5G connections. **6. Monitoring is reviewed annually (and dynamically)** Under the MGL Computing Policy, web filtering **and monitoring systems** are reviewed at least **annually**, with a clear change-control system with MGL for tightening or relaxing settings based on safeguarding evidence. Monitoring is also **dynamically reviewed** whenever safeguarding patterns arise (CPOMS analysis, DSL/briefer meetings, computing observations). This satisfies the DfE’s requirement for **continual improvement** rather than a “set and forget” model. **7. Monitoring is proportionate and privacy-aware** The AUP ensures: • monitoring is used **only for safeguarding**, not surveillance

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• access to monitoring logs is restricted to authorised leaders • decisions follow data-protection principles (necessity, minimisation) This meets DfE expectations around proportionality and ethical use of monitoring technologies.
Appropriate monitoring – If you use a pro/active technical monitoring solution, has the provider filed a submission to the UK Safer Internet Centre? – Have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations? – Have you satisfied yourself that your filtering provider meets the items on the checklist offered by the Safer Internet Centre? – How does monitoring respond to but also feed into the curriculum (e.g. lots of captures on issue X might lead to lessons being reordered) and into proactive safeguarding interventions for whole groups?	🟩			Banks Road Primary's monitoring strategy is **appropriate, proportionate and age-suitable** for a primary school context. The school balances safeguarding vigilance with privacy, ensuring that monitoring is *not excessive*, is *clearly understood by staff*, and is *integrated with curriculum and pastoral approaches*. Monitoring is therefore **effective without being intrusive**, meeting DfE Standard 4 in full. **1. Proportionate monitoring based on need, age and risk** Monitoring at Banks Road is designed specifically for primary-aged pupils: • Monitoring focuses on **patterns of risk**, harmful search attempts, and unsafe behaviour signals rather than tracking everything a child does. • Controls are appropriate for younger learners who require **higher protection** online (e.g., blocking of social media, chat platforms, mature content). • DSL and leadership ensure monitoring does **not become surveillance**, in line with the AUP's data-minimisation expectations.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			This proportionality aligns strongly with DfE guidance. **2. Blended monitoring: technical + human insight** Banks Road uses a **dual monitoring system**, which is considered best practice for primary settings: **Technical monitoring** • Internet activity logs, blocked-content attempts, and search patterns are surfaced for DSL review. • Alerts are only generated when necessary, ensuring signal-not-noise. • MGL supports configuration and annual review to ensure settings reflect risk without over-monitoring. **Human monitoring** • Teachers closely supervise pupils in lessons, using live marking and questioning to spot unsafe use instantly. • PSHE/Computing lessons reveal understanding gaps through scenario discussion (e.g., group chats, image-sharing). • Pastoral staff identify patterns from conversations, friendship fallouts or disclosures (common in KS2). This blended model ensures monitoring is **developmentally appropriate and contextual**, not purely technical. **3. Monitoring tied directly into safeguarding systems** Monitoring is appropriate because it is **purpose-specific**:

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			it exists solely to safeguard children. • When monitoring flags a concern, staff must notify the DSL *same day*, and the incident is recorded in **CPOMS**. • DSL triages risk, contacts parents, and initiates support or referrals as needed. • Monitoring insights influence **curriculum delivery**, **assemblies**, and **parent communication**. This integration ensures monitoring is used responsibly, consistently and proportionately. **4. Monitoring boundaries strengthened by BYOD and device controls** Monitoring is only effective if pupils cannot bypass it. Banks Road ensures: • Pupils cannot use personal devices or mobile data on site (*“no use, no sight, no sound”*). • All online activity takes place on school-managed, filtered and monitored devices. • Visitors and staff must not use personal devices with pupil data or pupils in view. This ensures the monitoring system remains **comprehensive and reliable**, while still proportionate. **5. Curriculum input ensures pupils understand what monitoring is for** The school ensures pupils understand monitoring in an age-safe, non-threatening way:

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• Computing units teach pupils how safe searching, privacy and reporting work (e.g., Y4 *Smarter Searching*, Y6 *Social Media & Being Safe Online*). • RSHE teaches pupils to recognise risks, understand boundaries and report concerns until they are heard. • PSHE focuses on kindness, respectful communication and peer influence—including **online relational behaviour**, preparing pupils to use technology appropriately. Monitoring is therefore **normed within a protective curriculum**, rather than hidden. **6. Monitoring decisions guided by ongoing risk intelligence** Banks Road uses **real-world patterns** to shape appropriate monitoring: • Online Safety Newsletters address trends such as inappropriate language in group chats or impersonation—indicating monitoring is **real-issue-led**, not generic. • DSL CPOMS analysis highlights which year groups or cohorts need additional teaching or monitoring focus. • Annual review with MGL ensures monitoring evolves with safeguarding landscapes. This ensures monitoring settings remain **proportionate and evidence-based**.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**7. Data protection & privacy considerations** The AUP makes clear that: • monitoring access is restricted to authorised safeguarding leaders • monitoring is used only for safeguarding or operational integrity • logs are not used for staff performance evaluation or unnecessary surveillance This ensures monitoring protects children without infringing on privacy more than necessary.
Limitations – With most providers there will be some activity that cannot be viewed, or instances where it is much more difficult to track who is using a device. What are these limitations and what mitigations (e.g. more restrictive access) or manual controls (e.g. a physical log of who uses which ipad in a lesson) are in place? – Are staff aware of whether keywords only are monitored, if these are set in context, whether images are screened or not, whether context can be given etc. – What is in place for devices in the home and BYOD if applicable? – What physical / real time monitoring of screens takes place, when and how (e.g. a teacher walking around and watching screens, or some schools have a live view of a whole class set of screens etc)? How do you avoid too many false positives making the system unusable? – How are staff encouraged to help the team by flagging if they are planning e.g. a lesson that will bring lots of flags (e.g. a poem that mentions death or suicide, research into wars or an RSHE lesson on		🟨		Even with robust filtering, proportionate monitoring, strong classroom supervision and clear policies, **no system provides absolute protection**. Banks Road Primary is transparent about these limitations and manages them within a safeguarding-first framework. **1) Scope & coverage** • **School systems only**: Technical monitoring can only see activity on **school-managed devices/services**; it cannot see what happens on personal devices on mobile data, nor activity at home, clubs or in the community. Your Mobile Phone Policy reduces this risk on site (*“no use, no sight, no sound”*), but off-site use remains outside direct monitoring. **Mitigation**: keep the school day device-free for pupils; keep parent comms frequent and practical (e.g., newsletters on chats, privacy, reporting) so that oversight extends to home.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
sex or intimate body parts etc)?		🟨		• **Authorised connections only**: BYOD is not allowed onto curriculum/admin networks by default; any visibility of such devices is limited unless explicitly approved and configured. **Mitigation**: maintain strict approvals/change-control; reiterate to staff/visitors that personal devices must not process pupil data or connect without authorisation. **2) Technical constraints** • **False negatives & "new" risks**: Filters/monitoring rely on **known lists, signatures, and rules**; newly emerging sites, slang, coded language, or novel AI-supported behaviours may not be immediately detected. The MGL model does include **regular updates/annual review**, but there is always latency. **Mitigation**: preserve a rapid tuning route (Computing Lead/DSL/SBM → Headteacher → MGL) and embed curriculum content that builds pupil *self-protection* when technology lags. • **False positives & over-blocking**: Protective settings can occasionally block legitimate curricular resources, creating short-term disruption and teacher frustration. **Mitigation**: use your documented **whitelist** pathway (with audit trail) so teachers can regain access swiftly while safeguarding remains primary.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
		🟨		• **Signal vs noise**: Monitoring that is too "chatty" becomes unmanageable; settings must remain **proportionate** to keep alerts actionable (DfE expectation). Your AUP positions leadership/DSL to calibrate this, but tuning is an iterative task. **Mitigation**: termly DSL reviews of patterns (CPOMS + logs) and small, evidence-led adjustments rather than broad, frequent reconfigurations. **3) Human factors** • **Attempted bypass or concealment**: Pupils can learn to hide tabs, use euphemisms, or move risky conversations to **unmonitored group chats** outside school hours. **Mitigation**: curriculum + RSHE explicitly teach refusal skills, reporting routes, and the permanence/impact of language and image-sharing; parent newsletters coach families to *see the chats*, review privacy, and exit unsafe groups. • **Staff vigilance varies**: Human monitoring is powerful, but attention can dip at busy moments. Your Assessment Handbook expects **in-the-moment feedback and supervision**, yet this remains a people dependency. **Mitigation**: keep classroom routines tight (devices face-down/closed when teacher speaks; clear "screens down" cue); use the visualiser to model safe choices; continue brief refreshers in staff meetings.

Question	Fully In Place	Partial / Needs Review	Not In Place	- Evidence/details (e.g. documents, training, reminders) & dates
		🟨		**4) Privacy & proportionality boundaries** - **Not surveillance**: Monitoring must remain **necessary and proportionate** (AUP). Leaders deliberately restrict access to logs, and the system is used **only** for safeguarding/operational integrity—not for broad user surveillance. This means not all low-level behaviour is visible or recorded by default. **Mitigation**: maintain clear "what to report" guidance; use CPOMS consistently for all safeguarding-relevant digital incidents; continue to educate pupils to self-report and seek help early. **5) Dependency on third-party services & configuration** - **Provider limits**: Efficacy depends on MGL platform uptime, rule set updates, and change-control throughput. While the SLA sets expectations and annual review is built in, performance can still be affected by vendor maintenance windows or industry-wide spikes in threats. **Mitigation**: keep a local "teaching contingency" (offline activities; pre-downloaded resources) and a simple, named escalation contact tree for urgent MGL tickets. **6) Off-site realities & the home environment** - **Home configurations vary**: Parental controls,

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
		🟨		router filtering, device settings, and supervision differ widely; younger siblings or older relatives may share devices; not all families apply 13+ rules consistently. Newsletters help, but the school cannot enforce home settings. **Mitigation**: continue frequent, practical communications (e.g., “how to check chats tonight”), link to platform guidance, and invite families to seek support early if online issues begin to affect learning/wellbeing. **7) Curriculum-monitoring gap** • **Understanding ≠ behaviour**: Pupils can “pass” unit checks (e.g., *Staying Safe Online*) yet still choose unsafely in real contexts. The curriculum validates knowledge; monitoring may not capture **intent** or **private choices**. **Mitigation**: spiral key messages (privacy, consent, reporting) across PSHE/RSHE; use scenario tasks and discussion to surface values and peer influence; act on pastoral disclosures promptly. **8) Evidence & logging constraints** • **Incomplete artefacts**: Staff are rightly told **not** to view/copy illegal images; sometimes all that is available are brief descriptions or reports, not screenshots/URLs. That can limit investigation detail. **Mitigation**: follow the AUP strictly—secure the device where necessary, **do not** view illegal

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
		🟨		content, inform the DSL, and involve police as required; record the chronology in CPOMS. **9) Time lag between incident and response** • **Real-time vs retrospective**: Technical alerts may be near-real-time, but some patterns only emerge **retrospectively** (e.g., repeated blocks). Pastoral fallout from out-of-hours chats typically appears **after** the event. **Mitigation**: same-day DSL notification culture; quick pastoral check-ins; targeted assemblies the same week; short “hot fix” messages to parents via ClassDojo when a pattern appears. **10) Change-management overhead** • **Friction by design**: Requiring approvals to open sites (to avoid unsafe access) introduces **lead time** that can pinch spontaneous classroom ideas. **Mitigation**: encourage staff to flag needs **ahead of units** (e.g., week-before whitelisting), maintain a shared list of “approved digital tools,” and review it termly. Banks Road’s controls are **strong and multi-layered**, yet the school is realistic about inherent limitations: **coverage ends at the school boundary; new risks appear faster than rules can update; people and privacy boundaries matter**. Your mitigations—tight device rules, curriculum that builds judgement, a

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
		🟨		responsive DSL/CPOMS workflow, termly pattern reviews, and steady parent education—keep residual risk **as low as reasonably practicable** in a primary setting.
Monitoring training – If using a pro/active solution, has your technical team attended training to understand exactly how it works, how it is set up and what the options are in order to inform a strategic approach and implement DSL/SLT requirements? – Has your safeguarding team attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what monitoring can/should do to inform the approach?	🟩			Banks Road Primary provides **well-structured, repeated and high-quality training** to ensure that all staff understand: • what online monitoring is • how the school's monitoring systems operate • what concerning digital behaviours look like • **how to respond and escalate immediately** • how monitoring feeds safeguarding (CPOMS → DSL → response) • their role in the DfE Filtering & Monitoring Standards This ensures monitoring is not a technical function alone, but a **whole-staff safeguarding responsibility**. **1. Whole-staff training that explicitly covers monitoring systems** **Filtering & Monitoring Training – MGL (15/04/24)** All teachers received formal training from MGL covering: • staff responsibilities under updated KCSIE • understanding filtering *and* monitoring • what a monitoring incident looks like • cyber-incident response • practical steps for staff when a monitoring alert

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			or concerning online behaviour occurs This is one of the strongest pieces of evidence that staff understand what monitoring is—and what it is **not**. **Training outcomes** Staff now: • understand how to interpret blocked-content attempts • know what "red flags" look like in digital behaviour • can take **immediate in-the-moment action** • know when to escalate to the DSL • understand monitoring logs as safeguarding intelligence **2. Cyber Security Training reinforces monitoring practice** **Cyber Security Training – whole staff (29/09/25)** Delivered by MGL, this session built staff awareness of: • digital-risk indicators • data-breach signals • system misuse • safe use of AI tools • how staff behaviour can compromise or strengthen school monitoring systems This training enhances staff understanding that monitoring systems form part of broader **cyber-resilience**, not just online safety.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**3. Whole-school safeguarding training strengthens monitoring response** Annual safeguarding training (e.g., **13/10/25**, **07/10/24**, **27/10/23**) includes monitoring-aligned content such as: • how to recognise online safeguarding concerns • how to respond "in the moment" • how to report *all* digital concerns immediately to the DSL • how CPOMS is used to record monitoring-led issues Because filtering is only one layer of protection, this training ensures staff can **spot behavioural signs** that monitoring tools may not detect. **4. Leadership-level training ensures oversight of monitoring systems** **Smoothwall Safeguard Briefing – DSL (05/10/23)** The DSL received advanced training from Smoothwall on: • industry monitoring standards • interpreting logs • setting thresholds • responding proportionately **DSL Refresher Training (annually)** Repeated annually (e.g., **22/09/25**, **23/09/24**, **19/09/23**) and includes digital safeguarding issues, threshold decisions, and monitoring responsibilities. This gives leadership the knowledge required to supervise monitoring activity, interpret concerns and implement

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			system changes via MGL. **5. Prevent & radicalisation training supports monitoring of extremist risk** Staff have undergone Prevent training across multiple years: • **15/09/25** (whole staff) • **10–11/03/25** (teachers/TAs) • **27/10/23** This ensures staff understand: • extremist content • radicalisation risk indicators • keywords/search patterns that may trigger concerns • how to escalate through DSL + CPOMS This is essential because DfE expects monitoring systems to *support* the Prevent duty. **6. Online Safety CPD supports understanding of monitored risks** Banks Road regularly trains staff on online risk behaviours that monitoring may reveal: • **Online Safety: The Essentials (11/11/25)** – signs of harm, how to recognise digital abuse, how to respond • **Online Safety Training – whole staff (08/05/24)** – apps to watch for, concerning language, block attempts

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			This aligns staff awareness with monitoring systems, ensuring behavioural cues and monitoring alerts are understood together. **7. CPOMS & escalation training embedded across all years** Monitoring is only effective if concerns move quickly into safeguarding processes. Your training log shows CPOMS reporting procedures embedded into: • **annual safeguarding training** • multiple staff meetings across years This results in: • rapid DSL notification • accurate digital-incident logs • data to inform future monitoring configuration and curriculum planning **8. Monitoring training for pupils (behavioural awareness)** Banks Road makes pupils part of the monitoring ecosystem through: • Digital Community Police Officer workshops (Years 3–6) • UK Safer Internet Centre events • Online Safety Days • anti-bullying workshops including cyberbullying content

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			Pupils learn: • why monitoring exists • what safe online behaviour looks like • how to report concerns to trusted adults This helps monitoring to detect **less** because pupils behave **more safely**. **Summary** Banks Road's monitoring training is: • **comprehensive** – whole staff, DSL + SLT, pupils • **technical + safeguarding integrated** • **externally quality-assured** (MGL, Smoothwall, PREVENT, SIP) • **documented and evidenced** • **recurring annually** This fully meets the DfE requirement that schools must ensure all staff understand how monitoring works, what it can and cannot detect, and how to act when concerns surface.
System configuration, customisation and review – Do your technical and safeguarding teams meet to discuss your monitoring needs and ensure systems are configured for the devices and systems you used and regularly updated/reviewed where changes are made and new devices added to ensure no devices or systems are missed? – How does the annual review and regular checks feed into settings and issues looked for on the monitoring system? This includes safeguarding teams requesting new items (e.g. keywords, particular	🟩			Banks Road Primary operates a **tightly governed, safeguarding-led configuration model** for all digital systems. Every platform, device, app or AI tool goes through a formally defined process of **approval → configuration → monitoring → review**, ensuring that technology use is safe, appropriate, legally compliant and aligned with curriculum intent. System configuration and review at Banks Road is **multi-layered**, combining technical expertise (MGL), safeguarding oversight (DSL), operational governance

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
users) to be added for flagging when mentioned or to see all activity responding to concerns, trends or incidents? – Are systems customised for your safeguarding needs – e.g. adding keywords that represent new concerns in your school/area or to follow students at particular risk. Is this approach documented and the system regularly reviewed to ensure appropriate access, settings and usage / do your policies reflect practice in school and are they updated when settings / approach are changed?	🟩			(SBM, Headteacher), and policy controls (AUP, AI Policy, Computing Policy). **1. All systems are configured through a strict, documented approval process** No digital tool or platform enters the school ecosystem without following the AUP-mandated approval route: **Staff request → Computing Lead → DSL/SBM risk check → Headteacher approval → MGL technical configuration** This prevents: • unsafe or unfiltered apps being installed • shadow IT • staff using tools without safeguarding sign-off • platforms with communication functions bypassing controls • unverified AI tools entering the school The AI Policy adds an **extra safeguard** through the AI Register: AI tools must also pass data-protection, ethical and safeguarding checks before approval. **2. MGL configures systems to meet safeguarding, security and curriculum needs** MGL provides: • configuration of filtering categories, monitoring settings and school-specific permissions • device management and secure configuration • installation of approved software only

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	- Evidence/details (e.g. documents, training, reminders) & dates
	🟩			- firewall and network setup compliant with primary safeguarding requirements - maintenance, patching and updates under the SLA All configuration changes are: - **audited** - **safeguarding-informed** - **documented** - **implemented only after leadership sign-off** This ensures systems remain secure, age-appropriate and fit for curriculum use. **3. Customisation follows safeguarding principles, not convenience** Customisation is always safeguarding-first: - Communication functionality is disabled unless required and approved. - AI tools cannot store or use pupil data. - No cloud classrooms, pupil email accounts or messaging systems are used. - Device permissions and app-stores are locked down (MGL). - Personal devices cannot connect to the network or process data Customisation ensures that all technology is **closed, safe, controlled and predictable**. **4. Annual review of system configuration (Computing +**

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**AI + AUP + Filtering)** Banks Road conducts **multiple annual reviews** covering: **Filtering rules & digital infrastructure** Required under the MGL Computing Policy, which mandates **annual review of web filtering** and the Computing Policy itself. **AI system review** The AI Policy requires an **annual review of all approved AI tools** on the AI Register. **AUP review** Ensures changes in cyber-risk, safeguarding expectations, and DfE guidance are incorporated. **Leadership oversight via DSL/CPOMS** Patterns from CPOMS logs and monitoring data feed into configuration review meetings. This means the school's digital estate is never static—configurations evolve with risk. **5. Real-time (dynamic) review linked to safeguarding intelligence** Configuration changes are made **during the year** when patterns emerge. Evidence from training logs shows staff trained to spot: • concerning search terms • repeated filtering blocks • digital behaviour patterns • potential grooming, extremism or bullying indicators

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			When these occur: 1. Staff report to DSL immediately (AUP + safeguarding training). 2. DSL evaluates via CPOMS data. 3. DSL/SBM/Headteacher request configuration updates from MGL if needed. 4. MGL adjusts filtering/monitoring categories, permissions or access. This creates a **live, responsive configuration cycle**, consistent with DfE Filtering & Monitoring standards. **6. System configuration protects data, privacy and legal compliance** The AI Policy adds: • GDPR compliance checks for all tools • prohibition of entering pupil data into AI systems • requirement to cease use immediately and escalate if a data-integrity concern arises The AUP confirms: • staff may not store or process pupil data on personal devices • only approved systems may be used • role-based access control These controls form the basis of Banks Road's **cyber-secure configuration standards**. **7. Continuous training ensures configuration is used correctly**

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			Staff and leaders receive training on system configuration and use, including: • **Cyber Security Training (29/09/25)** – AI, data breaches, system use • **Filtering & Monitoring Training (15/04/24)** – what configuration means in daily practice • **Online safety essentials sessions** – recognising when configuration is blocking/hiding risk behaviours This ensures configuration decisions translate into **safe and consistent practice** across classrooms.
Reports – If using a pro/active solution, is the system set up in such a way that you have a manageable number of captures and are not overwhelmed and therefore at risk of missing key safeguarding alerts? – Do you also run reports to spot trends over time? – Are concerns fed into the safeguarding systems you use to capture manual/offline safeguarding concerns to complete the safeguarding jigsaw and not kept in a separate silo?	🟩			Banks Road Primary operates a **clear, robust and safeguarding-first reporting framework** for all digital activity. Reporting of online safety, filtering/monitoring activity and digital safeguarding issues is **consistent, timely and documented**, ensuring that risks are identified early, addressed quickly and used to inform system improvements. Reporting at Banks Road is *not* a technical function—it is a **whole-school safeguarding mechanism** involving staff, DSLs, SLT, MGL, governors, and parents. **1. Staff reporting duties are clear, trained and consistent** The AUP states that staff must **immediately report any online-safety concern or monitoring alert to the DSL**, and that safeguarding takes precedence over all other considerations. This responsibility is reinforced through: • annual all-staff safeguarding training (2025,

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			2024, 2023 etc.) • filtering and monitoring training (MGL, 15/04/24) • cyber-security staff training (29/09/25) which includes “what to do in a data breach.” • Online Safety Essentials training (11/11/25) focusing on signs of online harm and immediate action. As a result, all staff know: • what concerns look like (blocked searches, unusual behaviour, concerning language, patterns) • how to respond in the moment • how and when to escalate to the DSL • how to document concerns on CPOMS This meets and exceeds DfE expectations that *all staff* must understand and use monitoring/online-safety reporting routes—not just SLT. **2. CPOMS provides a secure, auditable safeguarding trail** All online-safety incidents are recorded on **CPOMS**, as set out in your Assessment Handbook. This includes: • concerning search terms • repeated filtering blocks • observed unsafe behaviour online • online peer conflict • disclosures relating to digital activity

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• AI misuse or impersonation concerns The DSL uses CPOMS to: • maintain a chronology • assess thresholds • decide on actions (parents, Early Help, MGL, Police) • share information with SLT/governors • inform curriculum adaptation where patterns emerge CPOMS therefore acts as the **central safeguarding log** for all digital activity. **3. Monitoring & filtering reports feed into safeguarding actions** Banks Road has a well-established process for responding to monitoring/filtering reports: 1. **Filtering or monitoring event occurs** 2. Staff or system flags issue → **DSL notified immediately** 3. DSL logs the concern on **CPOMS** 4. DSL evaluates safeguarding risk (Prevent, bullying, grooming, coercion, harmful content) 5. DSL & SLT decide follow-up actions 6. If configuration needs adjusting, DSL/SBM escalate to **MGL** via documented change-control route The training log shows staff are trained to recognise and act on these events promptly (e.g., Filtering & Monitoring

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			training 15/04/24; Online Safety training 08/05/24). **4. Technical reporting is managed through MGL** The MGL Computing Policy sets out that: • MGL manages filtering logs • MGL supports review of incidents and filtering alerts • MGL provides advice on technical anomalies or potential cyber issues • MGL participates in annual policy and filtering reviews Where technical reports suggest a pattern (e.g., repeated attempts to access a category), these are escalated to the DSL and SLT for safeguarding assessment. This ensures technical and safeguarding reporting remain aligned. **5. AI misuse or safety concerns are reported via the AI Policy route** Banks Road's AI Policy requires: • staff to cease use **immediately** and report to the Headteacher if they believe an AI tool poses a **data, security, privacy or safeguarding risk** • any misuse of AI-generated content to be treated as a **conduct concern** • the Headteacher/DSL to review concerns with MGL This gives the school an effective reporting structure for emerging technological risks.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**6. Safeguarding reports inform system reviews** Reports (monitoring logs + CPOMS patterns) feed directly into: • **annual filtering review** (MGL Computing Policy) • **AI tool review** (AI Policy) • **AUP updates** • **curriculum changes** (e.g., moving online-safety units earlier in the year) • **parent communications** via newsletters This ensures digital systems remain **dynamic and responsive** to real risk. **7. DSL and SLT produce internal safeguarding reports** The school produces termly safeguarding reports (required by AUP and DSL expectations), which include: • online-safety incidents • monitoring/filtering patterns • actions taken • needed curriculum adjustments • MGL technical changes These reports feed into: • SLT safeguarding briefings • governor oversight (Safeguarding/IT Governors) • school improvement planning This evidences strong governance around online safety and monitoring.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**8. Parents are kept informed appropriately** Although parents do not receive filtering logs, they do receive: • tailored Online Safety Newsletters • case-based reminders (e.g., group chat risks, privacy settings) • direct DSL contact where an incident concerns their child This ensures transparency without sharing sensitive safeguarding information.
Other – Please also consider the school devices when at-home / curriculum / BYOD questions mentioned in the filtering section above and add any aspects not already covered there.				
HOME / REMOTE LEARNING & DEVICES IN THE HOME				
School devices in the home – If you send school devices home with students, how are they protected / monitored? – Do you have internet filtering/monitoring on them? (NB the standards stress that checks for filtering & monitoring should include those used off site)? – Many schools will have less restrictive filtering at home – detail this here and how decisions were made/mitigations? – Are they locked down as 'managed devices' or equivalent, so software cannot be un/installed except by school admins?	🟩			Banks Road Primary School operates a **strict no-loan policy** for school devices. Pupils are **not permitted to take school-owned iPads, laptops, Chromebooks or any other digital equipment home** under any circumstances. This approach is intentionally safeguarding-led and supports secure management of school systems, data and filtering controls. This stance is consistent with your whole-school ICT expectations, safeguarding policies, and digital infrastructure: • The **ICT Acceptable Use Policy** requires that school devices are used on the school's secure, filtered and monitored network, and that

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			personal data must not be processed on unmanaged systems. School devices leaving site would reduce the school's control over filtering, monitoring, data security and appropriate use. • The **Mobile Phone & Smart Device Policy** reinforces a culture in which school-managed devices and systems remain within the supervised school environment. Pupils' personal devices are strictly prohibited on site, which also aligns with not issuing school devices for home use. • The **MGL Computing Policy** highlights the need for appropriately managed devices, updated filtering systems and secure handling of digital equipment. Maintaining school devices on-site ensures that filtering stays effective, up-to-date, and within the control of your technical partner. **Safeguarding rationale** Because safeguarding risks increase significantly when devices leave the controlled environment of the school, not issuing devices for home use ensures: • school filtering and monitoring are always active • technical oversight by MGL remains intact • pupils cannot access harmful or inappropriate content through school-owned hardware • parents are not placed in a position of responsibility for devices configured for school-only use • school systems, credentials and data remain protected

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			This zero-loan model eliminates several risk categories identified in the DfE Online Safety standards—including unmanaged Wi-Fi, home network vulnerabilities, inadequate filtering, and USB/digital contamination risks. **Remote learning expectations** In the event of remote learning being required (e.g., illness, individual isolation), the school provides **learning tasks that do not require a school device**. Home access is designed so that: • materials can be completed on paper or through parent-managed devices • no child is required to use a personal device if this would be unsafe or inappropriate • safeguarding expectations for home devices are communicated regularly through online-safety newsletters, RSHE curriculum and ClassDojo **Support for families** Although devices are not loaned, Banks Road supports parents by: • sharing clear advice on safe device use at home • promoting age-appropriate platform rules • guiding families on privacy, parental controls and respectful digital behaviour • encouraging parents to report online concerns that affect wellbeing or school life (via DSL/CPOMS routes)
Live lessons (most schools deliver scheduled <u>and unexpected</u> live lessons (e.g. open days, elections, snow days, broken boilers, etc.) – Do you have a home/remote learning policy or clause in another	🟩			Banks Road Primary School does **not** deliver live lessons in any form — including video calls, streamed teaching, real-time online classrooms, or remote face-to-face

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
policy that covers behaviour for pupils and staff? – What key safeguarding precautions are included? – Where are they logged?	🟩			digital instruction. This is a deliberate safeguarding and operational decision, aligned with school policies and the protective digital environment maintained for pupils. This approach is consistent with: • the **ICT & Internet Acceptable Use Policy**, which restricts staff from using personal devices, personal communication tools or unapproved digital platforms for any school-based communication or teaching activities • the **Mobile Phone & Smart Devices Policy**, which ensures that pupils do not have access to personal devices or communication apps during the school day and reinforces tight boundaries around digital contact between staff and pupils • the **MGL Computing Policy**, which positions school devices, filtering, and supervision as systems designed specifically for **on-site, supervised** digital learning—not for remote video-based teaching **1. Safeguarding Rationale for No Live Lessons** Banks Road's decision not to use live lessons is grounded in safeguarding principles: **a) No controlled device environment at home** Because pupils do **not** take school devices home and home networks are not monitored or filtered by the school, live video-based lessons would place children online in an **unregulated environment**, without the technical protections required. **b) No safe platform that fits Banks Road's policies**

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			The AUP prohibits staff from using: • personal devices • unapproved apps • personal accounts • direct digital communication with pupils These restrictions are incompatible with live remote teaching models. **c) Privacy and data-protection risk** Live lessons can expose: • children's homes and family members • other pupils' identities • sensitive information through unintended audio or video capture These risks cannot be sufficiently mitigated without major infrastructural systems the school has chosen not to adopt. **d) Behaviour and safeguarding oversight** Live remote teaching would prevent staff from maintaining the high-level supervision, pastoral awareness and in-the-moment safeguarding vigilance that make classroom teaching safe and effective. **2. Remote Learning Model Used at Banks Road** If remote or home learning is required (e.g., illness, individual absence), the school provides **offline or asynchronous tasks** that do not require live digital interaction, such as: • paper-based learning packs

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• printable or view-only materials • assignment tasks posted via parent communication routes (e.g., ClassDojo), not child accounts • optional parent-supported resources This ensures children are not placed in an unsupervised online video environment and staff do not engage in prohibited one-to-one or live digital contact. **3. Staff Conduct and Accountability** Staff are **not permitted** to: • deliver curriculum content via live video • hold remote calls with pupils • send pre-recorded lessons to individual children • use personal devices or apps for teaching or contact Any request or suggestion for live lessons is directed to the **Headteacher and DSL**, and the standard response is that live lessons are **not part of the school's safeguarding-compliant model.**
	🟩			**4. Communication with Families** Parents are regularly reminded (via ClassDojo, AUP references, and online-safety newsletters) that: • the school will **never ask** a child to join a live video call • no teacher will contact a child directly via video, chat, or personal messaging

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• remote learning tasks will always be routed through **parent channels**, not pupil accounts This avoids confusion and removes opportunities for impersonation or unsafe digital contact.
Homework / cloud platforms accessible from home (all other platforms that can be accessed at home, whether for homework or during home learning) – Are these covered in policies and AUPs and regularly updated as new platforms/systems are bought? – Are all systems audited to ensure that they have an audit trail, central administration not limited to one person, oversight of administrators and settings locked down where features are not required, e.g. to not allow unmonitored communications?	🟩			Banks Road Primary sets **online homework only through specific, whitelisted services** (e.g., **maths.co.uk**; **Times Tables Rock Stars / NumBots**), accessed by pupils at home via parent-managed devices. **We do not use cloud-based classroom platforms** (no pupil email domains, shared drives, VLEs, or live/recorded lessons) and we **do not loan school devices**. This keeps the model simple, safeguarding-led, and aligned with our ICT Acceptable Use, Mobile Phone, and MGL Computing policies. **Key operating principle:** Homework platforms are used **only** for practice and curriculum reinforcement (e.g., number facts, arithmetic, set tasks). No direct messaging, file-sharing, or child-to-staff digital contact routes are enabled in our setup. **1) What we use, and why** • **maths.co.uk** and **TTRS/NumBots** are used to reinforce taught skills at home through short, structured practice. Tasks are set by teachers and completed on a home device under parent oversight. There are **no school cloud drives, pupil email accounts, or remote classroom spaces** attached to these tools in our model. (This mirrors the AUP requirement to avoid unapproved platforms and to keep

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			communication channels tightly controlled.) • Because pupils **do not take school devices home**, these activities run **outside** the school’s filtering/monitoring perimeter; hence our strong emphasis on **parent guidance** and clear boundaries around school–home contact. **2) Safeguarding expectations for home access** • **No staff–pupil direct messaging** via homework sites; teachers set tasks only. Any question or concern must come **via parents** using approved school channels (e.g., office/ClassDojo parent messaging, never child accounts). This aligns with the AUP’s prohibition on unapproved digital contact and personal devices/apps. • **Parent supervision** is encouraged: sit nearby for younger children, check privacy settings, and ensure platforms used are the school-specified ones. Our **Online Safety Newsletters** routinely give practical “do-this-now” tips (e.g., review group-chat membership, check who can add/message your child), which apply broadly to home device use around homework time. • **No live/recorded lessons** and **no cloud classroom**: families should never be asked to join video calls, upload recordings, or share personal files. If a child receives such a request purporting to be from school, parents should report it to the DSL immediately.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**3) Data protection and account management** • **Minimal, role-based accounts**: Where logins are required (e.g., TTRS/NumBots), we provide **pupil-only credentials** for practice. Staff must **not** use personal email or devices to set or track homework, and pupils must **not** submit personal information on third-party sites beyond what the school has enabled. (Matches AUP requirements on access controls and data minimisation.) • **No storage of pupil data on home devices**: Parents are advised not to save passwords in shared browsers and to keep devices updated, with basic parental controls where available—advice reinforced through our newsletters. **4) Curriculum fit and teacher practice** • Homework consolidates the **in-school curriculum** (e.g., number facts, arithmetic fluency), with expectations sequenced across year groups (see Computing/PSHE online-safety strands for safe search and respectful behaviour, which we revisit in class so pupils can apply them at home). • Teachers record concerns that affect learning/wellbeing (e.g., a child reports unkind messages during homework time) using **CPOMS** and follow the DSL escalation routes, even if the issue originated off-site. (This mirrors the assessment/safeguarding workflow described in the Assessment Handbook.)

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**5) Communication with families** • We **only** use parent-facing channels to share homework information; children are **not** contacted directly online by staff. This avoids ambiguity and aligns with our **no BYOD/no live lessons** stance and the AUP's restrictions on communication routes. • Newsletters and ClassDojo updates provide **practical safety prompts** tied to real trends (e.g., group-chat language, impersonation) that may surface around homework time on home devices. **6) Support and troubleshooting** • If a site is **down** or a login fails, teachers will provide **paper alternatives** or non-device tasks—no pupil will be disadvantaged for technology problems. This reflects our **no-cloud, no-loan** design and keeps homework equitable. • Any suspected phishing, fake homework messages, or requests to use unfamiliar apps should be reported to school immediately; staff will verify and respond through approved channels (AUP reporting expectations).
GENERAL – ALL TECHNOLOGY USED IN / BY THE SCHOOL				

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
Safeguarding & technical collaboration and review – Do safeguarding and technical teams review at least annually (or whenever significant changes are made to technology or the way the school works or new technologies are adopted), which platforms, systems and devices are used, what due diligence is completed to check their safety and suitability, what their settings allow and why, plus risks and mitigations? NB-not just filtering/monitoring. – Are generative AI tools covered in this? What is allowed/not/by whom/when and why? What are the risks and mitigations? What is your process for agreeing which AI can be used? Are staff familiar with this process? – When you do your 'regular checks' of filtering/monitoring (we recommend half termly, which other systems are checked/reported on at the same time by IT teams to senior leaders / DSLs? – In 2025 are you paying particular attention to any software (not just websites) which may give access to generative AI tools? Do these meet the Jan 25 DfE 'Generative AI: product safety expectations' and do you have regard to DfE document 'Generative artificial intelligence (AI) in education'?	🟩			Banks Road Primary maintains a **high-trust, high-safeguard** digital environment by ensuring that *every* technology used in school—devices, platforms, filtering systems, AI tools, software and apps—is overseen through **joint safeguarding and technical governance**. This collaboration ensures that tech adoption, configuration and ongoing review always prioritise **child protection, data security, staff conduct expectations, and curriculum integrity.** This safeguarding-technical partnership operates across several interconnected layers: **1. Senior leadership oversight & safeguarding responsibility** The **Headteacher and DSL** hold strategic responsibility for all technology adoption, usage, and monitoring across the school. This includes: • evaluating all digital tools (including AI systems) for **safeguarding risk** • ensuring compliance with national frameworks, data protection law and DfE Online Safety Standards • ensuring technology never replaces safeguarding vigilance, supervision or face-to-face pedagogy The ICT Acceptable Use Policy also makes clear that leadership must understand filtering/monitoring systems, approve platform use, and manage escalation for risks or breaches.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**2. MGL technical partnership: filtering, security and AI compliance** The school's ongoing service relationship with **MGL** provides: • **filtered and protected internet access**, reviewed annually to ensure pupils cannot access inappropriate or harmful content • technical advice on the **security, data handling, and appropriateness** of any technology or AI tool being considered • support for DSL/SBM/Computing Lead in resolving questions around system integrity, cyber-risk, or new tool evaluation The AI Policy states that MGL contributes to **evaluation, trial, data security checks and regular updates** of AI tools used by staff, including data-handling and storage compliance. This joint model ensures safeguarding and technical oversight are **not siloed**. **3. Joint evaluation of all AI tools before adoption** Your AI Policy sets out a **formal, safeguarding-led review process**: • A **register of approved AI tools** is maintained by the Headteacher. • Staff may *only* use AI tools that have been reviewed and approved through this process. • Any request to use a new AI tool must be evaluated for:

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			○ data protection compliance ○ safeguarding risk ○ curriculum relevance ○ alignment with school values and pedagogical approaches • MGL supports the technical evaluation, and the DSL ensures safeguarding is prioritised. This meets and exceeds DfE expectations for **due diligence** on third-party technology. **4. Annual review cycles with safeguarding at the centre** Across all your technology policies (ICT AUP, MGL Computing Policy, AI Policy), there is a consistent expectation of **annual safeguarding review** of: • filtering systems (annual review required) • monitoring configuration (DSL/SBM oversight) • all approved AI tools (annual review of the AI register) • curriculum delivery tools and apps This process ensures: • filtering remains age-appropriate • monitoring remains proportionate • data-protection expectations remain current • new threats are identified and addressed • AI tools remain compliant with governance and ethical standards The AI Policy explicitly states that approved tools will be

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**reviewed annually**, and new requests must be evaluated within **20 working days**, adding rigour and timeliness to the system. **5. Safeguarding controls built into all technology use** Across your policies, safeguarding standards underpin *every* digital scenario: • **No student data** may be shared with external platforms without verification and compliance checks. (AI Policy + AUP) • **No personal devices** used to process pupil information. (AUP + Mobile Phone Policy) • **AI-generated content** must be clearly labelled and fact-checked; misuse is a staff conduct breach. (AI Policy) • **Monitoring and spot-checking** of AI use is carried out by the Headteacher and DHT • **Technical behaviour** (filtering/monitoring logs, attempted access, unsafe usage patterns) informs safeguarding decisions through CPOMS. (AUP + Assessment Handbook) All technology therefore sits inside a **protective safeguarding perimeter**. **6. Collaboration between staff, DSL, Computing Lead and MGL** Banks Road's digital governance model is highly collaborative: • Staff raise concerns or requests to the

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			DSL/Computing Lead. • The DSL evaluates safeguarding risk. • The SBM manages operational considerations. • MGL evaluates data integrity, security and technical capabilities. This collective model ensures that **no technology is used in isolation**, and no staff member is expected to navigate technical or safeguarding complexities alone. **7. Safeguarding-aligned implementation and ongoing compliance** The AI Policy provides a clear compliance structure: • CPD for all staff on approved tools • spot-checks by the Head and DHT • line manager oversight of any AI-generated content before distribution • governor involvement through the Chair of Governors (IT Governor) This type of accountability is unusual in primary schools and demonstrates advanced practice.
Communication functionality – Have you identified all platforms allowed for use in school which have a chat function e.g. Scratch, Bandlab, Padlet etc (do review this regularly as new features get added to products/apps)? Have you enforced any safety controls related to these? – Are all platforms that include any chat function (remember that ‘comments’ can be used to chat, especially if they are never monitored) included in your policies, AUPs and risk assessments and locked down in the way your school wants them?	🟩			Banks Road Primary maintains **tight, safeguarding-driven control** over all communication functionality available through school technologies. This applies to *all* digital tools, devices, platforms, AI systems and apps used by staff or pupils. Communication features—messaging, chat, email, comments, file-sharing, video, audio, uploads or AI-powered conversational elements—are **strictly limited**, **centrally controlled**, and **risk-assessed** before adoption.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
NB – any gen AI site may have this functionality – Are all staff and pupils aware which platforms they can use to communicate between pupils or between staff and pupils and that they must never use accounts/emails/apps that are not approved/linked to the school?	🟩			This ensures the school fully complies with DfE Online Safety Standards regarding communication channels and prevents unsafe digital contact, misuse, or unmonitored conversations. **1. No pupil-to-pupil or pupil-to-staff digital communication systems** Banks Road does **not** provide pupils with: • email accounts • messaging systems • chat functions • collaborative cloud platforms • commenting tools • live or pre-recorded video platforms This design choice prevents: • unmonitored private messaging • inappropriate content-sharing • digital misconduct or harassment • impersonation or contact from unknown parties This aligns with the **ICT Acceptable Use Policy**, which prohibits staff from using personal communication tools with pupils and restricts communication to approved parent-facing channels. The **Mobile Phone Policy** strengthens this by preventing pupils' personal devices—and therefore apps like WhatsApp, Snapchat or gaming chats—from being used on site.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**2. Staff-to-pupil communication is *never* digital** The school enforces a **zero digital contact** rule between staff and pupils: • No emails to pupils • No messaging • No calls • No video interactions • No AI-mediated communication tools • No communication via homework platforms All communication flows **through parents**, never directly to children. The **AI Policy** reinforces this by banning the use of AI tools for any communication that could involve or identify pupils, and prohibiting entry of any pupil data into AI tools. **3. Parent-to-school communication restricted to approved, monitored channels** Parents communicate with the school through: • the school office • ClassDojo *parent accounts* (never child accounts) • formal letters / email routed through official accounts • meetings with staff Parents and pupils **cannot** contact staff through: • personal email • personal devices

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• social media • unapproved messaging apps This matches the ICT AUP and Mobile Phone Policy, which explicitly forbid staff giving personal contact details or engaging with parents or pupils via personal platforms. **4. AI systems have communication functionality disabled or restricted** Your **AI Policy** puts powerful safeguards around AI tools used in school: • Only **approved AI tools** (ChatGPT, TeachMate AI, Microsoft Copilot) may be used—and only by staff, not pupils. • Staff **must not** enter personal data or pupil information into AI tools. • AI tools cannot be used for **communication with pupils, parents or external parties** unless the Headteacher authorises a specific, reviewed use case. • All AI-generated content must be **clearly labelled**, fact-checked and ethically compliant. • Any AI functionality offering chat, conversation, or dynamic messaging is permitted **only for staff use** (e.g., workload reduction) and only under controlled conditions. This ensures AI cannot introduce **new, unmonitored communication routes**. **5. No communication-enabled homework or cloud**

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**platforms** Banks Road deliberately avoids cloud classroom systems that include: • messaging • chat • shared editing • video • comments • collaboration tools Homework platforms (e.g., **maths.co.uk**, **TTRS**, **NumBots**) are **practice-only** environments without communication channels. Pupils cannot send messages, upload files, or contact teachers. This eliminates the single largest communication vulnerability seen in many schools. **6. Communication functionality disabled or restricted on all devices and apps** Through the MGL SLA, all school-managed devices and apps have: • blocked chat features • locked-down user accounts • no app-store installation rights • no social media access • no unauthorised email Filtering and monitoring systems prevent access to: • social media communication

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• open chatrooms • gaming chat • messaging platforms • unsafe forums This keeps the school communication ecosystem **closed, safe, and staff-supervised**. **7. Communication-related incidents feed into safeguarding and curriculum** Any communication-related concern—e.g.: • group chat issues outside school • inappropriate language online • impersonation in gaming chats • digital fallouts ...is reported immediately to the DSL and logged on CPOMS. The DSL uses these patterns to: • adjust curriculum (RSHE / PSHE / Computing) • update parents through newsletters • review monitoring or filtering controls This ensures communication risks are addressed **proactively**.
Technology in your policies / AUPs – Are the latest school system, platforms and devices that **CAN** be used/accessed at home included in your policies/AUPs etc? – Have these been updated/audited recently to ensure they are still accurate? – Are the rules possible to follow (e.g. systems named which no longer	🟩			Banks Road Primary embeds technology expectations **consistently and explicitly** across all core policies, ensuring that safeguarding, behaviour, data protection and curriculum design are all aligned to the same standards. Across the AUP, Mobile Phone Policy, AI Policy, MGL Computing Policy and RSHE Policy, the

Banks Road Online Safety Audit & Risk Assessment

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
exist or “use a school camera” when they don’t exist or work)? – Where is your photo/video policy stored? When was it last updated? – What is your approach to checking the setting’s devices regularly to ensure imagery and content is appropriate? Who does this? How often? What do they check? Do you check/ clear the photo gallery/ camera roll?	🟩			school maintains a **coherent, low-risk, safeguarding-first digital environment**. The result is a policy suite where: • staff know what technology they *can* and *cannot* use • pupils understand boundaries and expectations • parents receive clear, consistent messages • all devices, systems and platforms operate within clear governance structures • data, privacy and safeguarding are protected at every stage **1. ICT Acceptable Use Policy (AUP): the foundation for all technology behaviour** The AUP provides the **core governance** for all digital activity in the school. It explicitly defines: **Clear roles & oversight** The AUP assigns responsibility for filtering and monitoring oversight to: • **Headteacher** • **DSL** • **School Business Manager** • **MGL technical partner** These leaders must understand the systems and respond to concerns appropriately. **Staff expectations** The AUP prohibits: • use of personal devices for processing pupil data

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• staff–pupil digital contact • sharing personal contact details or social media links • introducing unapproved software, apps or cloud platforms **Reporting routes** All concerning digital incidents must be reported immediately to the **DSL** and recorded on **CPOMS**, ensuring safeguarding visibility. The AUP is therefore the “spine” that supports all other technology policies. **2. Mobile Phone & Smart Devices Policy: school-wide boundary setting** Banks Road’s Mobile Phone Policy establishes **clear, simple, enforceable rules**: • Pupils: **no use, no sight, no sound** at any time on site • Phones handed in and stored safely where permitted • Staff: restricted use, *never* in the presence of pupils, and never for processing pupil data • Visitors: no photos, no device use around pupils This policy removes the largest BYOD safeguarding risk: **unfiltered, unmonitored mobile data**. It also reinforces the AUP by preventing communication routes and data-handling behaviours that contradict safeguarding expectations.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**3. AI Policy: rigorous governance for AI systems** Banks Road's AI Policy is unusually strong for a primary setting. It provides: **Clear ethical and safeguarding boundaries** • AI must **never** replace face-to-face teaching. • No pupil data may be entered into AI tools. • Deepfakes, impersonation, grooming risks and harassment must be explicitly taught to pupils. **Formal approval model** • The Headteacher maintains a **register of approved AI tools**. • Staff must request permission before adopting any new AI system. • MGL jointly evaluates tools for data security, compliance and safeguarding. **Compliance monitoring** • Headteacher/DHT complete **spot checks**. • AI content must be **labelled** and **fact-checked**, with misuse treated as a staff conduct breach. This creates a policy environment where **innovation never compromises safeguarding**. **4. MGL Computing Policy: technical alignment with safeguarding** The MGL Computing Policy provides the technical backbone for school systems: • Web filtering is kept **up-to-date** and reviewed annually.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• Teachers must maintain records of formative/summative computing assessment. • External devices and tools must be risk-assessed before use. • The Computing Lead and CP Officer jointly ensure **online safety remains a high priority**. It reinforces the AUP and AI Policy by ensuring **technical controls** support safeguarding controls. **5. RSHE Policy (2026): curriculum-embedded digital safeguarding** Your RSHE Policy ensures that technology expectations embedded in the AUP are **taught explicitly** to all pupils: • respectful online behaviour • privacy, boundaries, age restrictions • risks linked to image-sharing and permanence • how to recognise AI manipulation (deepfakes) • how to report unsafe online behaviour until they are heard This ensures policy is not abstract—pupils learn *why* these expectations exist. **6. Consistency across all school policies** Across the full policy suite, there is **no contradiction** in the expectations placed on technology use. All policies reinforce: • safeguarding-centred decision-making • zero tolerance for unsafe communication routes

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• no personal device use for school data • no digital contact between staff and pupils • careful evaluation of new tools (AI + tech change-control) • robust filtering + monitoring oversight This consistency is a major strength and ensures all staff understand boundaries. **7. Staff training, compliance & accountability** Technology expectations in policies are reinforced through: • staff induction and CPD • line-management oversight for AI use • spot-checks by SLT • leadership approval for new tools • CPOMS safeguarding trails Policies do not sit on a shelf—they are **active, implemented and monitored**.
CYBERSECURITY				
Audit , documentation and standards (given its importance for continuity of access to systems and data for keeping children safe, schools secure and maintaining continuity of teaching & learning, cybersecurity should be audited separately) – Does your school have the 3 documents recommended by the National Cyber Security Centre? ○ cybersecurity policy ○ risk + asset registers ○ incident response plan	🟩			Banks Road Primary operates a **documented, standards-aligned cybersecurity framework** that integrates safeguarding, data protection, technical controls, and governance processes across all digital systems. The school's approach is consistent with DfE *Meeting Digital and Technology Standards*, the UK GDPR, and sector-level expectations for cyber hygiene, access control, data minimisation, and system oversight. Cybersecurity auditing and documentation are

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
– Are these accurate and regularly updated, read by all and reflected in practice?	🟩			embedded in multiple policies—not siloed—ensuring the school maintains a *single, consistent governance environment*. **1. Formal annual review cycles of all digital systems** Across your technology policies, annual review is a **mandatory requirement**, providing a structured audit cycle: • **Filtering systems reviewed annually** as per the MGL Computing Policy, ensuring that updates to web-filtering rules reflect current risk. • **Computing Policy reviewed annually**, including cybersecurity provisions, digital infrastructure, device governance and safeguarding links. • **AI Policy reviewed annually**, alongside an annual review of all approved AI tools. This includes security, privacy, ethical compliance and updates from MGL. • **AUP and safeguarding documentation reviewed annually**, including technical access control and data-handling expectations. This ensures the school's cybersecurity posture is kept current and aligned with evolving threats, product changes, software updates and DfE guidance. **2. Documented responsibilities, governance and accountability** The school's policies assign clear roles for cybersecurity management:

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• **Headteacher, DSL & SBM**: responsible for understanding filtering/monitoring systems, reviewing digital safety, overseeing data-protection compliance and leading incident response. • **MGL technical partner**: responsible for system maintenance, web-filter updates, infrastructure support, and providing technical assurance on AI tools and data storage procedures. • **Chair of Governors (IT Governor)**: participates in decision-making on adoption and monitoring of AI tools, representing governor-level scrutiny. Cybersecurity governance is therefore multi-layered, documented and backed by both educational and technical expertise. **3. Documentation of all technology approvals and risk assessments** Banks Road maintains **formal documentation** for technology approval, including: **AI Technology Register** • A controlled list of all approved AI tools, maintained by the Headteacher. • Each tool must undergo a documented risk-assessment process covering: ○ data protection ○ safeguarding ○ curriculum relevance ○ security compliance

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			○ technical integrity (via MGL) ○ ethical considerations **Change-control pathway for digital tools** The AUP and MGL Computing Policy require that any request to use new digital tools, apps, online services or platforms follows a documented approval route: **Staff → Computing Lead → DSL/SBM review → Headteacher sign-off → MGL configuration** This prevents unaudited or unsafe systems from entering the school environment. **4. Clear documentation of standards for safe data handling** Cybersecurity expectations around data protection are explicitly documented in the AUP and AI Policy, including: • **GDPR compliance checks** for all AI tools before approval. • Prohibition on entering **any pupil data** into external systems (AI tools, third-party platforms) without verification. • Restrictions on use of **personal devices** to store, process or access sensitive information. • Requirement to end the use of any digital system immediately and escalate if there is a concern about data integrity or security. • Enforcement of **access controls**, ensuring staff only access the digital data they need. These documented standards prevent data leakage, unauthorised access and unsafe digital behaviour.

QUESTION	**FULLY IN PLACE**	**PARTIAL / NEEDS REVIEW**	**NOT IN PLACE**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**5. Integration with safeguarding audit processes (CPOMS)** Cybersecurity incidents or digital concerns are recorded through **CPOMS**, forming part of the documentation that supports safeguarding audit trails: • All online-safety concerns are logged with chronology and evidence. • DSL reviews patterns and actions termly and during PPM cycles. This ensures cybersecurity concerns feed directly into safeguarding governance, not treated in isolation. **6. Technical audit support via MGL** The MGL Computing Policy outlines MGL's responsibilities for: • annual web-filter audit • technical updates and patching cycles • infrastructure checks • data-storage compliance • professional evaluation of new systems The AI Policy adds an additional layer—MGL must provide **regular review and update information** related to AI tools' data-storage or handling risks. This ensures the school's entire digital estate is subject to professional, documented technical assurance. **7. Policy-driven adherence to national cybersecurity**

Question	Fully In Place	Partial / Needs Review	Not In Place	- Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**expectations** Although not explicitly referencing Cyber Essentials, Banks Road implicitly adheres to DfE cybersecurity standards by documenting: • restricted admin privileges • tight BYOD and device-use controls • approved-platform lists • mandatory reviews • staff conduct restrictions • clear technical–safeguarding escalation processes These measures meet the spirit of: • **DfE Meeting Digital and Technology Standards** • **UK GDPR requirements** • **NCSC fundamentals for schools (access control, filtering, monitoring, patching)**
Standards Are you aware of and meeting the Cyber Security standards for Schools and Colleges published by the DfE (updated in 2025), which are referred to in KCSIE?	🟩			Banks Road Primary aligns cybersecurity to a **standards-based framework** that is proportionate for a primary setting and tightly integrated with safeguarding. In practice, the school implements the spirit and requirements of: • **DfE "Meeting Digital and Technology Standards"** (secure access, filtering & monitoring, governance, patching, device management, continuity). These expectations are embedded in the AUP and MGL Computing Policy (leadership oversight of filtering/monitoring; annual reviews; controlled change; approved tools only).

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• **DfE Filtering & Monitoring Standards** (leadership ownership; annual review; age-appropriate protection; proportional monitoring). These are operationalised through named roles (Headteacher/DSL/SBM), SLA with MGL, and the annual review cycle for filtering and platforms. • **UK GDPR and data-protection principles** (lawful basis, minimisation, access control, security by design). These are enforced through the AUP (no personal devices for pupil data; role-based access; reporting duties) and the AI Policy's prohibition on entering pupil data into external/AI tools. • **NCSC-aligned good practice** (least privilege, patching, malware protection, restricted admin rights, network segregation). While not named explicitly, the MGL Computing Policy reflects these through managed devices, web-filtering updates and SLA-driven maintenance; the AUP restricts installation/unauthorised software and enforces approvals for any new tool or connection. Together, these standards give Banks Road a **clear operating model**: protect by default; approve and review centrally; minimise data; embed safeguarding; and document everything material in CPOMS and policy reviews. **1) Governance & Risk Management (Leadership**

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**Standards)** • **Named roles and accountability:** The AUP assigns filtering/monitoring oversight to the **Headteacher, DSL and SBM**, with MGL as the technical partner—ensuring decisions about risk and configuration remain safeguarding-led. • **Annual review & assurance:** The MGL Computing Policy requires an **annual review of web filters** and policy; the AI Policy mandates **annual review of all approved AI tools**—providing a recurring risk-assessment cycle across the digital estate. • **Change-control:** Any new digital/AI tool follows a documented route (Staff → Computing Lead → DSL/SBM → Headteacher → MGL), preventing shadow IT and ensuring configuration aligns with safeguarding and data protection duties. **2) Access Control & Acceptable Use (People Standards)** • **Least privilege & controlled access:** Staff access only what they need; personal devices **must not** be used to process pupil data; introducing unapproved software or platforms is prohibited. • **Staff–pupil digital boundaries:** No direct digital contact with pupils via email/chat/video; communications route **via parents only** through approved channels—reducing impersonation and social-engineering risk.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• **AI conduct & transparency:** Only **approved AI tools** may be used by staff; all AI-generated materials must be **labelled and fact-checked**; breaches may trigger staff-conduct processes. **3) Technical Controls (Technology Standards)** • **Filtering & monitoring:** Professionally managed web-filtering under SLA; age-appropriate blocking with monitoring alerts and DSL escalation; annual reviews to keep rule-sets current. • **Device and software governance:** Managed school devices; installation rights locked down; no unapproved apps; obsolete/broken kit handled in line with data-protection expectations. • **Data protection in AI:** Data handling/storage of AI tools reviewed with MGL; **no pupil data** entered into AI systems; cease use and escalate if any data-integrity concern arises. **4) Documentation & Evidence (Process Standards)** • **Policy documentation:** AUP, MGL Computing Policy and AI Policy capture the standards, the roles, and the procedures for approvals, incident response, and review cycles. • **Safeguarding records:** All online-safety incidents and cyber-related concerns (e.g., suspicious access attempts, harmful searches) are documented in **CPOMS**, creating an

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			auditable safeguarding trail that feeds leadership/governor oversight and curriculum adjustments. **5) Education, Culture & Continuous Improvement (Practice Standards)** • **Staff awareness & compliance:** Expectations reinforced via induction/INSET, line-management sign-off for AI use, and SLT **spot-checks** to ensure compliance with approval, labelling and data-handling rules. • **Safeguarding-cyber loop:** Cyber signals (filter logs, pattern alerts) trigger **DSL action** and **curriculum reinforcement**; patterns and actions appear in CPOMS and in termly leadership/gov updates—closing the loop between technology and safeguarding practice.
Technical staff – Do technical staff have training on cybersecurity and report to senior leaders and governors on issues, mitigations incidents and training needs?	🟩			Banks Road Primary does not use an internal IT technician model. Instead, the school implements a **hybrid safeguarding + technical support structure** where: • **MGL** provides specialist technical services, system maintenance, filtering, security configuration and technical assurance. • **In-school leaders** (Headteacher, DSL, SBM, Computing Lead) provide safeguarding governance, digital conduct enforcement, and technology-risk oversight. This creates a model that is **low-risk, tightly controlled and fully aligned to DfE Cybersecurity Standards**,

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			ensuring all technical changes occur under **expert supervision + safeguarding scrutiny**. **1. MGL as the school's technical authority** The **MGL Computing Policy** establishes MGL as the school's designated technical support provider, responsible for: • maintaining and updating filtering systems • ensuring web filters remain compliant, secure and age-appropriate • providing advice on data integrity, security and storage • supporting infrastructure maintenance, device management and patching • advising on the technical viability, risk and compliance of new tools (including AI) MGL's role is therefore not only operational but also **critical to the school's cybersecurity assurance**. **2. Technical collaboration with safeguarding oversight** The AUP makes clear that filtering and monitoring oversight is held by: • **Headteacher** • **DSL** • **School Business Manager** • **MGL technical team** This ensures that: • MGL manages the technical infrastructure

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• Safeguarding leaders manage interpretation, escalation and risk • All configuration changes (e.g., whitelisting, access requests, new tools, AI approval) require **joint approval** This model prevents technical decisions from being made without safeguarding visibility. **3. Change-control responsibilities** All requests for new digital tools, websites, software or AI systems follow a **documented change-control process**: **Staff → Computing Lead → DSL/SBM (safeguarding check) → Headteacher (authorisation) → MGL (technical implementation)** MGL only implements changes once safeguarding and leadership have approved them, ensuring: • no "shadow IT" • no unsafe or unfiltered apps enter the environment • no technical configuration occurs without curriculum and safeguarding alignment This is a strong cybersecurity control and unusual in primary settings. **4. MGL's role in AI safety & compliance** The **AI Policy (2025)** explicitly names MGL as the school's technical advisor for AI systems, responsible for: • reviewing data-storage and handling risks • ensuring systems meet GDPR and international

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			data-legislation standards • advising on adoption decisions • supporting the Headteacher/DSL when concerns arise This ensures AI is introduced **safely**, ethically, and with expert oversight. **5. Technical incident support & escalation** Cyber-related threats (e.g., repeated blocked access attempts, concerning activity, suspected compromise) follow a three-tiered response: 1. **Staff → DSL** (safeguarding triage & CPOMS recording) 2. The **DSL/SBM** evaluate whether a system/configuration issue is present 3. **MGL** is contacted for technical diagnosis, resolution and security assurance This combined approach ensures incidents are treated as **both** safeguarding concerns **and** cybersecurity events. **6. No direct pupil or staff access to high-risk technical functions** Among your policies: • Staff do **not** have rights to install software, modify systems, adjust security settings or bypass filtering. • Pupils have **no device-level control** and cannot add apps, configure settings, or access app stores.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			• AI systems may only be used by staff, and only after approval; pupils cannot use AI tools. This drastically reduces cybersecurity exposure. **7. Governors included as part of the technical governance structure** The AI Policy requires the **Chair of Governors (IT Governor)** to be involved in decision-making relating to the adoption and use of AI tools. This means governors play a direct role in: • ensuring compliance • maintaining oversight • scrutinising technical and data-handling risks —another strong safeguard for accountability and cyber resilience. **8. MGL supports compliance with national standards** While not labelled “Cyber Essentials”, your MGL-supported configuration covers the same foundations: • role-based access • restricted admin rights • secure configuration & patching • web filtering & monitoring • managed devices • secure decommissioning This embedded model effectively meets the DfE *Technology Standards* and NCSC cyber hygiene

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			expectations.
Training – Are <u>non-technical</u> staff given training and regular reminders on cybersecurity best-practice (passwords, phishing, reporting and more)? – Are students taught about cyber security and how to keep their accounts and data safe?				NCSC non-technical training for school staff is available for free, e.g. from LGfL https://booking.lgfl.net/book/add/p/33 Training is also available for governors here: https://lgfl.bookinglive.com/book/add/p/160 The NCSC also have resources available here: https://www.ncsc.gov.uk/information/resources-for-schools
DATA PROTECTION				
– Do you have a clear data protection policy in place that meets requirements regarding UK GDPR? – Who is your Data Protection Officer in your setting? – If you have CCTV, is there a robust policy that ensures you comply with data protection legislation? – Who has access to the recordings from CCTV? How is this managed to safeguard children? – As well as the many other considerations regarding generative AI tools, how/where have you made clear to staff what they are/are not allowed to do with school/staff/student data and what they are allowed to use gen AI tools for or not from a data protection perspective?	🟩			Banks Road Primary School has a robust, compliant and well-maintained data protection framework supported by up-to-date policies for data protection, data retention and CCTV. Evidence across all three policies demonstrates strong governance, secure systems, clear procedures and statutory compliance. **1. Leadership, Governance & Compliance** **Evidence:** • School is the **Data Controller**, formally registered, and meets GDPR/DPA 2018 duties. • A named **Data Protection Officer (DPO)** with independence and clear responsibilities is in place. • **Data Protection Assessor / Information Risk**

Question	**Fully In Place**	**Partial / Needs Review**	**Not In Place**	- Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**Lead (Jamie Wilson)** appointed with responsibility for risk and compliance. - **Information Asset Owners (IAOs)** for key systems are identified (SBM & Deputy Headteacher). - The Governing Board has defined oversight responsibilities, including CCTV audit twice per year. **2. Policies & Procedures** **Evidence:** - **Data Protection Policy (Apr 2025)** is comprehensive, covering GDPR principles, lawful processing, rights of individuals, security measures, breach management and privacy notices. - **Data Retention Policy (Feb 2026)** provides a full statutory retention schedule, secure disposal procedures, CPOMS expectations, legal holds and auditing requirements. - **CCTV Policy (Apr 2025)** ensures compliance with GDPR, lawful use, retention (30 days max unless required), signage, access controls and request processes. **3. Training & Staff Responsibilities** **Evidence:** - All staff must follow secure handling, storage and disposal rules, and comply with access control,

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			password, encryption, email, device and cloud guidelines. • Staff must report potential breaches immediately, with the Head and DPO carrying out statutory notifications. • CCTV policy outlines staff conduct expectations and disciplinary sanctions for misuse. **4. Data Management, Record Keeping & Retention** **Evidence:** • Statutory retention schedule includes: ○ **Safeguarding:** DOB + 25 years (or +75 years for CSA). ○ **Pupil records:** transferred to next school. ○ **Admissions/attendance, HR, finance, governance and H&S storage periods** all fully documented. • CPOMS used as secure safeguarding system with controlled access. • Secure archiving, legal holds and disposal logs are built into processes. **5. Rights of the Data Subject** **Evidence:** Policies clearly articulate rights to: • **Access (SARs)** with 1-month response and extension rules. • **Rectification, erasure, restriction, objection**

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			**and data portability**, aligned with GDPR. • CCTV policy includes formal application process for image access and safeguards for third-party privacy. **6. Security Measures, ICT Controls & Breach Management** **Evidence:** • Password, encryption, portable devices, off-site backup, firewall, MIS access and secure email protocols are detailed. • CCTV recordings stored securely with restricted access, authorised viewers only, and strict protocols for emergency viewing (two senior leaders). • CCTV retention period is **maximum 30 days** unless required by police or for disciplinary purposes. • Clear data breach procedures including ICO notification within 72 hours when required. **7. CCTV Use, Data Handling & Access** **Evidence:** • CCTV used for crime prevention, safety, property protection and welfare. • Overt cameras only; covert CCTV prohibited except in exceptional circumstances. • Access controlled through: ○ **Application form for public requests**

QUESTION	**FULLY IN PLACE**	**PARTIAL / NEEDS REVIEW**	**NOT IN PLACE**	• Evidence/details (e.g. documents, training, reminders) & dates
	🟩			○ **Emergency access protocol requiring two senior leaders** ○ **Police requests via Data Protection Controller** ○ **Governor audits twice per year** • Signage meets legal expectations and is placed in relevant locations.