

INKBERROW PRIMARY SCHOOL

ONLINE SAFETY POLICY



Our commitment

Online safety is a whole-school safeguarding responsibility. We protect and educate pupils, equip staff and families, and respond promptly whenever technology contributes to a concern.

Document control	Details
Policy owner	Headteacher / Designated Safeguarding Lead / Computing Lead
Approval body	Academy Standards Committee (ASC)
Approval date	17 th September 2026
Effective from	September 2026
Review date	September 2027, or sooner following statutory or material change
Trust	Quest Learning Trust

Love to Learn, Learn to Care

Contents

- 1. Policy statement, aims and scope
- 2. Statutory and national framework
- 3. Understanding online safety: the 4Cs
- 4. Roles and responsibilities
- 5. Our Online Safety Curriculum
- 6. Staff training and professional conduct
- 7. Working with parents and carers
- 8. Filtering, monitoring and technical safeguards
- 9. Acceptable use, mobile phones and smart technology
- 10. Generative artificial intelligence (AI)
- 11. Online communication, publishing and remote learning
- 12. Responding to online safety concerns and incidents
- 13. Specific online harms
- 14. Record keeping, monitoring and review
- Appendix 1: EYFS and KS1 acceptable use agreement
- Appendix 2: KS2 acceptable use agreement
- Appendix 3: Adult acceptable use agreement
- Appendix 4: Staff response pathway
- Appendix 5: Filtering and monitoring review record
- Appendix 6: Staff knowledge and training audit
- Appendix 7: Inky's Staying Safe Online poster
- Appendix 8: Governor assurance checklist

Approval record

Role	Name	Signature / minute reference	Date
Chair of ASC	Deborah Gardner		
Headteacher	Mr Duggan-Seville		

Key school contacts

Responsibility	Named person / arrangement
Headteacher and Designated Safeguarding Lead (DSL)	Mr Duggan-Seville
Deputy Designated Safeguarding Leads (DDSLs)	Mrs Janet McPherson, Mr. Ryan Coy, Miss Anne Hiley and Mrs Nicola Taylor
Pastoral Lead	Mrs Nicola Taylor
Online safety lead	The DSL
SLT lead for filtering and monitoring	The Headteacher / DSL
Responsible governor	Safeguarding governor – Deborah Gardner
Technical support	Quest Learning Trust and its approved IT support arrangements

Immediate concern

If a child is in immediate danger, call 999. Staff must report urgent safeguarding concerns directly to the DSL or a DDSL without delay and then make a factual CPOMS record. CPOMS must not be relied upon as the only alert for an urgent concern.

1. Policy statement, aims and scope

Inkberrow Primary School recognises that technology is integral to children's education and daily lives. It creates valuable opportunities to learn, communicate and participate, but it can also facilitate harm. Online and offline safeguarding cannot be separated: technology may be the place where harm occurs, a means by which it is facilitated, or a source of evidence about a wider safeguarding concern.

This policy sets out the school's whole-school approach to protecting and educating pupils, supporting staff and families, and identifying, intervening in and escalating online safety concerns. It is grounded in the four areas of online risk - content, contact, conduct and commerce - and is implemented alongside the Child Protection and Safeguarding Policy.

1.1 Aims

- safeguard pupils, staff, volunteers, visitors and governors when using connected technology;
- build pupils' knowledge, critical thinking, digital resilience and confidence to seek help;
- teach a progressive, age-appropriate Online Safety Curriculum from Reception to Year 6;
- recognise that some pupils, including pupils with SEND or other vulnerabilities, may face additional online risk or barriers to reporting;
- maintain proportionate technical protections without unreasonably restricting teaching and learning;
- set clear expectations for acceptable, safe, respectful and lawful use;
- respond consistently to concerns, preserve evidence appropriately and make referrals where required;
- work openly and constructively with parents, carers, Quest Learning Trust, technical providers and safeguarding partners; and
- review practice regularly because technologies, platforms and harms change rapidly.

1.2 Scope

This policy applies to all pupils, staff, governors, volunteers, contractors, visitors and community users of school systems. It applies to school networks, accounts, cloud services, devices and equipment; school-managed devices used off site; personal devices used for school business; remote education; and online behaviour beyond the school day where it affects safeguarding, welfare, relationships, discipline, the learning environment or the school community.

References to "technology" include computers, tablets, phones, watches, cameras, messaging and social media services, online games, livestreaming, search engines, cloud platforms, virtual or augmented reality, internet-connected devices and generative AI tools.

1.3 Principles

- The welfare of the child is paramount and being harmed is never the child's fault.
- Online safety is a running and interrelated theme across safeguarding, curriculum, behaviour, data protection, staff conduct and parental engagement.
- A culture of "it could happen here" is maintained. Concerns are listened to, taken seriously and acted upon.
- Pupils are taught how to recognise risk, make informed choices and seek help; technical controls do not replace education and supervision.
- Responses are child-centred, proportionate, non-blaming and informed by age, development, SEND, communication needs and the wider context.
- The school balances safeguarding, privacy, freedom of expression and access to a broad curriculum within the law.

2. Statutory and national framework

This policy has been updated for the guidance in force in England in September 2026. It has regard to:

- [Keeping Children Safe in Education 2026](#)

- [Relationships Education, Relationships and Sex Education and Health Education statutory guidance \(effective 1 September 2026\)](#)
- [Teaching online safety in schools](#)
- [Filtering and monitoring: core standard](#)
- [Cyber security standards for schools and colleges](#)
- [Generative artificial intelligence in education](#)
- [Mobile phones in schools](#)
- [Searching, screening and confiscation at school](#)
- [Sharing nudes and semi-nudes: advice for education settings](#)
- [Education for a Connected World](#)
- [Prevent duty guidance](#)

Relevant legislation includes the Education Acts 1996, 2002 and 2011; Education and Inspections Act 2006; Equality Act 2010; Human Rights Act 1998; Children Acts 1989 and 2004; Counter-Terrorism and Security Act 2015; Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025; Online Safety Act 2023; and legislation concerning communications, harassment, sexual offences, indecent images of children, fraud and computer misuse. This policy also reflects the academy trust's funding agreement, articles and delegated governance arrangements.

3. Understanding online safety: the 4Cs

The 4Cs provide the basis of the school's online safety approach. Risks frequently overlap, and an incident may fall into more than one category.

Area of risk	What it means at Inkberrow
Content	Being exposed to illegal, inappropriate or harmful content, including pornography; racism; misogyny; antisemitism; extreme sexual or physical violence; self-harm or suicide content; radicalisation and extremism; misinformation, disinformation, fake news and conspiracy theories; harmful challenges; and AI-generated or manipulated material.
Contact	Being subjected to harmful interaction with other users or generative AI applications that simulate interaction. This includes peer pressure, bullying, commercial advertising, unwanted contact and adults or children posing as someone else in order to groom or exploit a child sexually, criminally, financially or otherwise.
Conduct	Online behaviour that increases the likelihood of, or causes, harm. This includes abusive or threatening messages, online bullying, impersonation, exclusion, doxxing, non-consensual sharing, creating/sending/receiving explicit images (including AI-generated material), harassment and behaviour that damages another person's reputation or privacy.
Commerce	Risks arising from commercial activity, including inappropriate or targeted advertising, persuasive design, in-app purchases, loot boxes, online gambling or gambling-like features, scams, phishing, fraud, identity theft, subscription traps and financial exploitation.

Safeguarding lens

Staff do not treat the 4Cs as a checklist that limits professional curiosity. Online activity can reveal abuse, exploitation, neglect, mental health concerns, radicalisation, domestic abuse, child-on-child abuse or risk in the child's family or community.

4. Roles and responsibilities

4.1 Quest Learning Trust and the Academy Standards Committee

Quest Learning Trust is the proprietor. Through its governance and delegation arrangements, the Trust and Academy Standards Committee (ASC) provide strategic oversight and hold the Headteacher to account for implementation.

They will:

- ensure online safety is embedded across safeguarding and relevant policies;
- ensure appropriate filtering and monitoring systems are in place and receive assurance that the DfE standards are met;
- identify a responsible SLT member and governor for filtering and monitoring;
- ensure an effectiveness review is completed at least once every academic year by the responsible SLT member, supported by the DSL, IT support and responsible governor, with checks and actions recorded;
- receive proportionate information about trends, incidents, curriculum implementation, staff training and technical assurance without unnecessary personal data;
- ensure staff receive induction, regular training and at least annual safeguarding updates that include online safety and filtering/monitoring responsibilities;
- ensure teaching is appropriately adapted for vulnerable pupils and pupils with SEND; and
- review and approve this policy annually or sooner when required.

4.2 Headteacher

The Headteacher has operational responsibility for ensuring this policy is understood and implemented consistently. The Headteacher will allocate sufficient time, training and resources; ensure responsibilities are explicit; approve any exceptional and documented temporary changes to filtering; ensure technology procurement includes safeguarding, privacy and security assessment; and act on weaknesses or emerging risks.

4.3 Designated Safeguarding Lead and deputies

The DSL takes lead responsibility for online safety as part of the safeguarding role. This lead responsibility is not delegated, although activities may be supported by deputies and other colleagues. The DSL will:

- maintain knowledge of current online risks, local context, reporting routes and support services;
- understand the filtering and monitoring arrangements, check relevant reports and respond to safeguarding alerts;
- work with the Headteacher, responsible governor and IT support to review filtering and monitoring and provide assurance to governors;
- coordinate the safeguarding response to online concerns, including referrals to Children's Social Care, the police, Prevent/Channel, CEOP or other services where appropriate;
- ensure urgent concerns are acted on immediately and decisions, rationale, actions and outcomes are recorded;
- identify patterns, repeat concerns, vulnerable groups and curriculum or supervision needs;
- ensure parents/carers are informed unless doing so would place a child at greater risk, prejudice an investigation or be contrary to agency advice;
- support staff training and ensure lessons or visitors do not compromise safeguarding; and
- report appropriate anonymised themes and assurance information to the Headteacher and ASC.

4.4 IT support

Quest Learning Trust and its approved technical support arrangements are responsible for maintaining secure, reliable and appropriately configured systems. Technical staff/providers will work with the Headteacher and DSL to:

- maintain filtering, monitoring, identity and access controls, malware protection, backups, patching and secure configuration;
- apply required Internet Watch Foundation and counter-terrorism blocklists and prevent unauthorised circumvention;
- ensure controls apply to all relevant users, networks, school-managed devices and locations, including devices used off site where technically applicable;
- provide understandable reports and prompt support when safeguarding or security concerns are identified;
- test changes, new devices and services before deployment and record technical checks and actions;

- retain and disclose logs lawfully, proportionately and in accordance with data retention arrangements; and
- report any failure, suspected breach or material limitation immediately to the responsible SLT member and DSL.

4.5 All staff, volunteers and contractors

- read, understand and follow this policy, the Child Protection and Safeguarding Policy, Staff Code of Conduct and relevant acceptable use agreement;
- maintain appropriate professional boundaries and use only approved accounts, systems and communication routes;
- provide active supervision and teach safe, respectful and critical use whenever technology is used;
- recognise possible signs of online harm and maintain an attitude of “it could happen here”;
- know how filtering and monitoring work at the level needed for their role, report failures promptly and never attempt to bypass controls without authorised procedure;
- report safeguarding concerns directly to the DSL/DDSL and record them factually on CPOMS; and
- not investigate a possible crime, search a device without authority, or view/copy/forward sexual imagery.

4.6 Pupils

Pupils are expected to follow the age-appropriate acceptable use agreement, use technology kindly and responsibly, respect privacy and copyright, use only authorised accounts and services, protect passwords, and tell a trusted adult when something worries them or does not feel right. A child will not be blamed for reporting harm or for having been targeted.

4.7 Parents and carers

Parents and carers are expected to support the school’s acceptable use arrangements, model safe and respectful behaviour, talk regularly with their child about online life, use age-appropriate settings and supervision, and report concerns promptly. They should not investigate incidents between children, circulate allegations or contact another child directly through online channels.

5. Our Online Safety Curriculum

Inkberrow provides a planned, progressive Online Safety Curriculum from Year 1 to Year 6. The school uses its purchased National Online Safety programme, provided through The National College, alongside the Computing curriculum, SCARF PSHE, statutory Relationships and Health Education, assemblies and responsive teaching. The curriculum is revisited regularly rather than confined to an annual event.

Teaching is evidenced through curriculum planning, pupil work and class online safety floor books. Teachers assess understanding through discussion, scenarios, retrieval, pupil voice and application in other subjects. Emerging issues are taught responsively when they are relevant to pupils’ lives, while avoiding alarm, unnecessary detail or inadvertently directing pupils towards harmful content.

5.1 The eight areas of online safety

Curriculum area	Progressive learning focus
Self-image and identity	How online experiences shape identity and self-esteem; recognising idealised, manipulated or AI-generated representations; positive self-presentation; asking for help.
Online relationships	Respect, consent, trust, boundaries, peer pressure, strangers, grooming, healthy communication and safe help-seeking.
Online reputation	Digital footprints; permanence and circulation of information; how posts affect oneself and others; repairing mistakes.
Online bullying	Recognising bullying, harassment, exclusion and abusive behaviour; bystander responsibility; blocking, reporting, support and evidence.

Curriculum area	Progressive learning focus
Managing online information	Searching, evaluating sources, fact and opinion, algorithms, targeting, misinformation, disinformation, scams, persuasive design and AI outputs.
Health, wellbeing and lifestyle	Balanced use, sleep, physical activity, attention, emotions, harmful content, gaming and gambling-like features, and knowing when to seek help.
Privacy and security	Personal data, passwords/passphrases, privacy and location settings, phishing, fraud, permissions, secure accounts and reporting breaches.
Copyright and ownership	Ownership of creative work, permission, attribution, licences, lawful use, plagiarism and the intellectual-property implications of AI.

5.2 Curriculum implementation

- KS1 teaching uses concrete language, stories, role play and repeated routines: ask before going online, keep personal information private, be kind, stop/close/tell, and identify trusted adults.
- KS2 teaching develops critical judgement: privacy, digital footprint, manipulation, algorithms, scams, gaming and commercial pressure, respectful participation, reporting routes, age restrictions and the reliability of online or AI-generated information.
- UKS2 receives explicit, age-appropriate AI literacy and safety teaching, including generated or altered media, hallucinations, bias, privacy, intellectual property, responsible acknowledgement and why AI must not replace personal judgement.
- Pupils learn that the minimum age for most mainstream social media accounts is currently 13 and that age restrictions exist to reduce exposure to inappropriate content and unsafe contact.
- Lessons teach transferable knowledge and behaviours rather than relying on lists of current apps, because platforms and features change quickly.
- The same expectations of respect, honesty and consent apply online and offline, including when users are anonymous.
- Pupils rehearse how to report: stop, close or step away, do not respond or forward, and tell a trusted adult. Older pupils also learn appropriate platform reporting, blocking and trusted external routes.
- Online safety is reinforced whenever internet research, shared documents, email, media creation, gaming, AI or communication tools are used in other subjects.

5.3 Inclusion and safeguarding in teaching

Teaching will be adapted to age, developmental stage, prior experience, SEND, language, communication and vulnerability. Staff recognise that pupils with SEND may be more susceptible to online grooming, bullying, manipulation or misunderstanding, and may require explicit teaching, visual prompts, repetition, accessible reporting routes and individual safety plans.

If a lesson prompts a disclosure or concern, the member of staff will stop or adapt the activity as necessary, listen and follow safeguarding procedures. Personal experiences will not be solicited in public discussion. External visitors and resources will be checked in advance, remain under teacher oversight and be consistent with the school's safeguarding and curriculum responsibilities.

6. Staff training and professional conduct

All new staff, volunteers and relevant contractors receive online safety and filtering/monitoring information during induction. Staff receive safeguarding updates at least annually and more frequently when risks, systems or guidance change. Training includes the 4Cs, child-on-child online abuse, grooming and exploitation, sexual imagery, misinformation, radicalisation, AI and deepfakes, reporting routes, professional boundaries, data protection, cyber security, and each person's filtering and monitoring responsibilities.

The DSL and deputies update their online safety knowledge regularly and as part of their safeguarding training. Governors receive training sufficient to provide informed challenge and assurance. Technical staff receive role-specific training and work with safeguarding leaders so that alerts are interpreted in context.

6.1 Professional expectations

- Use school-approved accounts and platforms for work involving pupils or personal data.
- Do not communicate with pupils through personal social-media accounts, personal messaging services or gaming accounts.
- Do not accept pupils as contacts/friends or seek access to their private online spaces.
- Do not store school data on unauthorised personal devices, removable media or consumer cloud services.
- Use approved school equipment for images of pupils and follow consent, safeguarding and retention arrangements.
- Keep accounts secure, use unique strong passphrases and multi-factor authentication where provided, lock devices and report suspected compromise immediately.
- Maintain professional standards in all online activity. Personal online conduct must not compromise safeguarding, confidentiality, professional boundaries or confidence in the school.
- Refer media enquiries, online criticism, impersonation or threats involving the school to the Headteacher; do not respond personally.

7. Working with parents and carers

The school works in partnership with families and recognises that much of pupils' online activity takes place at home. Information is provided through newsletters, the website, workshops and National Online Safety/The National College resources. The school will communicate emerging issues proportionately and without naming children.

Parents and carers will be told, in accessible terms, about the school's filtering and monitoring arrangements; the platforms and sites pupils are asked to use; who pupils may interact with; the school's mobile-phone expectations; and how to raise concerns. The school encourages families to:

- talk regularly and without judgement about online experiences;
- use parental controls, privacy settings and age ratings while recognising that controls do not replace conversation and supervision;
- keep younger children's devices in shared spaces where practicable;
- review games, apps, livestreaming, chat and in-app purchasing features before use;
- protect passwords and personal/location information;
- agree healthy boundaries that protect sleep, activity, relationships and learning;
- save or screenshot ordinary abusive messages where safe and helpful, but never copy, save, print or forward nude/semi-nude or suspected illegal sexual material; and
- report urgent safeguarding concerns to school and contact police/CEOP as appropriate.

8. Filtering, monitoring and technical safeguards

Filtering is preventative: it blocks access to illegal, inappropriate or potentially harmful online material. The school uses

Monitoring is reactive: it identifies concerning activity for review and response. Neither is completely effective; they operate alongside curriculum, supervision, acceptable use, professional curiosity and prompt reporting. The school uses Senso.

8.1 Required arrangements

- Roles and responsibilities are identified for the ASC, responsible governor, Headteacher/SLT lead, DSL and IT support.
- Filtering and monitoring apply proportionately to all relevant users, school networks and internet-connected school-managed devices, including those used off site where technically applicable.
- Different profiles are used where needed for pupils, staff and guests. Unmanaged devices use a separate network where access is provided.
- Systems block illegal and harmful content, including required child sexual abuse and terrorist content blocklists, without unreasonably limiting teaching or pupils' opportunity to learn how to assess risk.

- The school considers images, video, audio, apps, dynamic/personalised content and AI-generated content, not only conventional webpages.
- Only authorised persons may approve temporary exceptions. The reason, scope, duration and safeguarding implications are documented, and the exception is removed promptly.
- All staff know how to report over-blocking, under-blocking, suspected circumvention, alerts and technical failure.
- Relevant monitoring alerts are reviewed by suitably trained staff and safeguarding concerns are escalated to the DSL without delay.

8.2 Annual and event-triggered review

The effectiveness of filtering and monitoring is reviewed at least once every academic year by the responsible SLT member, supported by the DSL, IT support and responsible governor. A further review takes place after a material safeguarding incident, new technology or generative AI product, major software/configuration change, new working practice, identified gap or significant change in pupil risk.

The review considers pupil age and needs, SEND/EAL, the school's risk profile, curriculum requirements, device and network coverage, off-site use, current blocking and alert arrangements, limitations, logs and incidents, staff knowledge, commercial and AI risks, and whether monitoring is effective and proportionate. Checks cover all relevant devices and locations and record the date, person, test, result and action. Appendix 5 provides a record template.

8.3 Cyber security and access management

- Accounts are individual wherever practicable and access is limited to what the role requires.
- Default or shared administrator credentials are not used for routine activity.
- Software, browsers, operating systems and security tools are patched and supported.
- Data is backed up and recovery arrangements are tested in line with Trust procedures.
- Phishing, malware, loss, unauthorised access or suspected data breach is reported immediately to the Headteacher/DSL, IT support and Data Protection Officer as applicable.
- Safeguarding and personal information is shared only through approved secure routes and retained in accordance with Trust schedules.

9. Acceptable use, mobile phones and smart technology

All users must follow the applicable acceptable use agreement. Use of school systems is primarily for education and authorised school business. Limited incidental staff use may occur only where permitted by Trust arrangements and must remain lawful, reasonable and professional. The school may monitor use lawfully and proportionately for safeguarding, security, operational and compliance purposes.

9.1 Pupils' personal devices

Inkberrow is a mobile-phone-free environment throughout the school day. Pupils do not have access to personal phones, smart watches with communication/camera functions or other personal connected devices during lessons, movement between activities, breaktime, lunchtime, clubs or other school-organised activities unless the Headteacher has approved an individual exception for medical, disability or safeguarding reasons.

Where Year 5 or Year 6 pupils need to bring a phone for the journey to or from school, it must be switched off on arrival and handed in or stored securely in accordance with the school's published routine. It must not be used until the pupil has left the school's care. Unauthorised use may result in confiscation and parental collection in line with the Behaviour Policy. The school will take reasonable care but families should avoid sending valuable devices unless necessary.

9.2 Searching and confiscation

Searching, screening, confiscation and examination of electronic devices will be undertaken only by the Headteacher or an authorised member of staff and in accordance with current DfE guidance, the Behaviour

Policy and the law. Staff will consider urgency, safeguarding risk, the pupil's cooperation, proportionality and whether material may be evidence of an offence.

If sexual imagery of a person under 18 is suspected, staff must not view, copy, print, screenshot, forward, save or ask a child to send it. The device should be secured without searching the content and the DSL informed immediately. The DSL will follow UKCIS guidance and police/social-care advice. Potential evidence must not be deleted.

10. Generative artificial intelligence (AI)

The school recognises the educational value of appropriate AI use and its safeguarding, ethical, data-protection, intellectual-property and reliability risks. AI services can generate convincing false information; reproduce bias; collect data; expose users to unsuitable outputs; simulate human contact; or be misused to impersonate, bully, groom, exploit or create altered images, deepfakes and sexualised material.

10.1 Safe and responsible use

- Only school-approved AI products, accounts and use cases may be used for school business or pupil learning.
- A proportionate risk, privacy, security and curriculum assessment is completed before a new AI product is introduced, including its age terms, data use, moderation, filtering/monitoring and ability to generate dynamic or personalised content.
- Personal, special-category, safeguarding, confidential or identifiable pupil/staff information must not be entered into a public or unapproved AI tool.
- Pupil-facing AI use is age-appropriate, purposeful and supervised. Children are not directed to create personal accounts contrary to service age requirements.
- AI output is treated as unverified. Staff and pupils check accuracy, source quality, bias and suitability and do not present generated work as independently created.
- Copyright, ownership, attribution and permitted use are considered. School and pupil work is not uploaded to train or prompt tools unless authorised and lawful.
- Professional judgement and responsibility remain with the human user. AI must not make safeguarding decisions, replace direct assessment of a child or be used as the sole basis for significant decisions.
- Any harmful, sexualised, threatening, discriminatory, impersonating or exploitative AI use is reported immediately and managed as a safeguarding concern.

11. Online communication, publishing and remote learning

11.1 Communication and social media

School communication with pupils and families uses approved channels and appropriate professional accounts. Access permissions, membership and moderation of shared spaces are reviewed. Staff do not use private/personal messaging with pupils. Any online group used for school activity must have a clear educational purpose, appropriate adult oversight and arrangements for reporting concerns.

11.2 Images, video and publication

Images and recordings are taken only for authorised purposes, on approved equipment and in accordance with consent, privacy, safeguarding and retention arrangements. Staff consider whether publication could reveal personal information, location, routines or vulnerability. Names and images are not combined unnecessarily. Livestreaming, video calls and public comments are risk assessed and moderated.

11.3 Remote education

- approved platforms and school accounts are used;
- staff-to-pupil contact follows professional-boundary and, where possible, auditable communication arrangements;
- joining details are shared securely and attendance/access is controlled;

- pupils and families understand expectations about location, clothing, backgrounds, recording and respectful participation;
- sessions are not recorded unless there is a defined, lawful and communicated purpose;
- staff report concerns arising during remote contact through normal safeguarding procedures; and
- reasonable adjustments are made so that safety arrangements do not exclude pupils with SEND or limited access.

12. Responding to online safety concerns and incidents

Online incidents are considered first through a safeguarding lens. Behavioural or technical consequences do not replace assessment of harm, vulnerability, coercion, exploitation, criminality, mental health, SEND or the need for support.

12.1 Expected staff response

1. Secure immediate safety and medical help. Call 999 if there is immediate danger or a crime in progress.
2. Listen calmly, take the child seriously, reassure them they have done the right thing, and do not promise confidentiality.
3. Use open prompts such as "Tell me what happened"; do not investigate or ask leading questions.
4. Report directly to the DSL/DDSL without delay for harm, risk of harm, sexual material/behaviour, grooming, exploitation, threats, self-harm/suicide concerns, radicalisation or possible crime.
5. Make a factual CPOMS record promptly, including the child's exact words, date/time, platform/device, witnesses, immediate action and who was informed.
6. Preserve potential evidence. Do not ask for harmful content to be forwarded. Do not view or copy sexual imagery.
7. Do not arrange mediation, compel an apology, contact an alleged user, or interview children together before the DSL has assessed risk and suitability.
8. Continue normal, calm support and follow any safety plan or agency advice.

12.2 DSL assessment and action

The DSL will consider the child's wishes and safety; the 4Cs; nature, content and circulation; age and development; power imbalance, coercion and repetition; SEND and communication needs; identity and protected characteristics; known adults/children; location and continuing access; possible criminality; risk to other children; and wider family/community context. The DSL will decide whether to manage internally, provide pastoral or curriculum support, seek Family Help, refer to Children's Social Care, contact police/CEOP/Prevent or seek specialist advice. Decisions and rationale are recorded.

Parents/carers are normally informed promptly and separately for each child. Contact may be delayed or withheld if it could increase risk, prejudice an investigation or conflict with statutory-agency advice. Support is provided to the child harmed, the child alleged to have caused harm and witnesses, without assuming guilt and without placing the burden of avoiding harm on the child harmed.

12.3 Reporting routes

Concern	Immediate route
School safeguarding concern	DSL/DDSL immediately; factual CPOMS record. In an emergency call 999.
Online child sexual abuse/grooming	DSL-led referral; CEOP where appropriate; police/Children's Social Care according to risk.
Nude/semi-nude image of a child	Do not view/copy/forward. Secure the device and contact DSL immediately; follow UKCIS guidance.
Illegal child sexual abuse material online	DSL/police response; Internet Watch Foundation reporting where appropriate.
Terrorist/extremist material or radicalisation	DSL; Prevent/Channel or police advice according to risk.

Concern	Immediate route
Fraud/phishing/cyber crime	IT support and Headteacher/DSL; Action Fraud/police and DPO as appropriate.
Data breach or lost device	Headteacher, IT support and Data Protection Officer immediately; preserve facts and follow Trust procedure.
Harmful public content	Platform reporting and UK Safer Internet Centre Report Harmful Content where appropriate, led by the DSL/Headteacher.

13. Specific online harms

13.1 Online bullying, harassment and prejudice

Online bullying may involve repeated intentional harm and an imbalance of power, but a single post, image or message may still cause serious harm and require safeguarding action. The school addresses abusive messages, exclusion, impersonation, rumours, humiliation, discriminatory content, misogyny, misandry, threats and pile-ons. Bystanders are taught to report rather than like, share or join in. Responses follow the Behaviour and Anti-Bullying policies alongside safeguarding assessment and support.

13.2 Child-on-child online abuse

Children can abuse other children through messaging, gaming, social media, shared documents, livestreams and AI tools. This may include sexual harassment, coercion to send images, non-consensual sharing, upskirting, threats, stalking, doxxing, deepfakes, encouraging self-harm or facilitating offline abuse. Such behaviour is never dismissed as banter or an inevitable part of growing up. The Child-on-Child Abuse Policy and KCSIE procedures apply.

13.3 Nude and semi-nude images, deepfakes and sextortion

Creating, requesting, possessing or sharing nude or semi-nude imagery of a child is a safeguarding concern, including self-generated, digitally altered, AI-generated or apparently synthetic material. Financially motivated sexual extortion ("sextortion") may involve threats to distribute imagery unless money, further images or actions are provided. Staff act immediately, avoid viewing or copying material, preserve devices and messages without forwarding content, and follow DSL-led UKCIS and police guidance.

13.4 Grooming and exploitation

Grooming can be sexual, criminal, financial, ideological or linked to trafficking and modern slavery. It may involve gifts, gaming currency, flattery, secrecy, threats, debt, fake identities or movement from public to private/encrypted channels. Staff consider whether a child is being coerced or controlled and whether other children are at risk. Victims may appear complicit or may have committed offences under pressure; this does not remove the need for protection.

13.5 Harmful content, self-harm, suicide and challenges

Content may promote self-harm, suicide, eating disorders, violence, dangerous challenges or hoaxes. Staff do not circulate the content or provide unnecessary detail. The DSL assesses immediate safety and mental-health risk, informs parents unless unsafe, seeks medical/emergency help where necessary and coordinates ongoing support. Whole-school communication avoids sensationalising or inadvertently signposting pupils to harmful material.

13.6 Radicalisation, extremism and hateful content

Online material and contact can normalise extremist narratives, prejudice or violence. Concerns are reported to the DSL and considered under the Prevent duty and Child Protection and Safeguarding Policy. Curriculum work develops respectful discussion, critical evaluation and understanding of manipulation while maintaining political impartiality and avoiding unnecessary exposure to harmful propaganda.

13.7 Misinformation, disinformation and manipulated media

Pupils are taught to pause, check provenance and purpose, distinguish fact/opinion, compare reliable sources, recognise targeting and emotional manipulation, and understand that images, audio, video and AI outputs can be convincing but false. Staff correct false claims without shaming pupils and report content that indicates safeguarding risk.

13.8 Commercial and financial harms

The curriculum and technical arrangements address advertising, influencer marketing, in-app purchases, subscriptions, loot boxes, gambling-like features, phishing, scams, fraud and identity theft. Pupils are taught not to make purchases, share payment details or respond to urgent financial requests without a responsible adult.

14. Record keeping, monitoring and review

Safeguarding concerns are recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy. Technical/security events are also reported through Trust IT arrangements. Records distinguish the child's account, observed facts, professional assessment, decisions, rationale and actions. Sensitive material is not attached unnecessarily; sexual imagery must never be uploaded to CPOMS.

The DSL reviews online-safety information for patterns, repeat users, locations, platforms, vulnerable groups, curriculum gaps and the effectiveness of actions. Governors receive anonymised assurance information at an appropriate frequency. Personal information is limited to those who need it and retained or disclosed lawfully.

This policy is reviewed at least annually by the Headteacher/DSL and ASC, and sooner following changes to law or statutory guidance, a serious incident, a material change in systems or working practice, introduction of new or AI-enabled technology, or evidence that arrangements are ineffective. The review is informed by pupil, staff and parent voice; curriculum evidence; safeguarding themes; training; annual risk assessment; and the recorded filtering and monitoring review.

14.1 Links with other policies

- Child Protection and Safeguarding Policy
- Child-on-Child Abuse Policy
- Behaviour Policy and Anti-Bullying arrangements
- Staff Code of Conduct and disciplinary procedures
- Data Protection Policy, privacy notices and records retention arrangements
- Computing, PSHE/RSHE and Remote Education policies
- Mobile Phone / Personal Device arrangements
- Photography, video and social media arrangements
- Complaints Policy
- Business continuity and cyber-security procedures

Appendix 1: EYFS and KS1 acceptable use agreement

My safe-use promise

Adults will help me use technology to learn. If anything worries me, I will stop, close the screen and tell a trusted adult.

Pupil name: _____ Class: _____

When I use a computer, tablet or the internet in school, I will:

- ask an adult before I begin and use only the apps, websites and accounts they have chosen;
- be kind and use the same good manners online as I use face to face;
- keep my full name, address, school, passwords and other personal information private;
- tell an adult straight away if I see something strange, upsetting or unsuitable, or if someone I do not know contacts me;
- not click pop-ups, links, downloads or messages unless an adult says it is safe;
- take care of equipment and tell an adult if something is broken;
- use only my own login and keep my password private; and
- stop, close the screen and tell a trusted adult if anything does not feel right.

I understand that adults may check how school technology is being used to help keep everyone safe.

Pupil signature (or agreed with an adult): _____ Date: _____

Parent/carers: I have discussed this agreement with my child and support the school's online-safety arrangements.

Parent/carers signature: _____ Date: _____

Appendix 2: KS2 acceptable use agreement

Pupil name: _____ Class: _____

I understand that using technology is a privilege and a responsibility. I will:

- use school technology, accounts, email, shared spaces, internet and approved AI only for the learning or activity an adult has authorised;
- use my own account, create a strong password/passphrase, keep it private and log out when finished;
- protect personal and location information belonging to me and others;
- communicate respectfully and never bully, threaten, exclude, impersonate or pressure another person;
- ask permission before creating, recording, uploading or sharing information, images or work about another person;
- pause and check before believing or sharing online or AI-generated information;
- respect copyright, acknowledge sources and explain honestly when approved AI has supported my work;
- not try to bypass filtering, use a VPN/proxy, change settings, install software or access another person's files;
- not search for, create, keep or share harmful, sexual, violent, hateful or illegal material;
- tell a trusted adult immediately about worrying content, contact, conduct or commercial pressure - even if I made a mistake or was told to keep it secret;
- not forward or save a nude/semi-nude image; I will close it and tell an adult; and
- keep any phone or smart device switched off and stored as the school requires throughout the school day.

I understand that school technology use may be filtered and monitored and that concerns will be managed to keep people safe. Consequences will be fair, proportionate and linked to the Behaviour Policy, but I will always be supported to report harm.

Pupil signature: _____ Date: _____

Parent/carers: I have discussed this agreement with my child, support the school's mobile-phone-free arrangements and consent to appropriately supervised use of school technology.

Parent/carers signature: _____ Date: _____

Appendix 3: Adult acceptable use agreement

Name: _____ Role: _____

I will:

- use school systems lawfully, professionally and primarily for authorised educational or work purposes;
- follow the Child Protection and Safeguarding Policy, Staff Code of Conduct, data-protection requirements and this policy;
- use approved accounts, devices, storage, communication and AI tools; maintain professional boundaries at all times;
- protect accounts with unique strong passphrases and multi-factor authentication where available; lock devices and keep them secure;
- access, use and share only the information I am authorised to handle, through approved secure routes;
- actively supervise pupils' technology use and check the suitability of content, links and services before use;
- report safeguarding concerns directly and immediately to the DSL/DDSL and record factually on CPOMS;
- report filtering/monitoring failures, cyber incidents, lost devices, phishing and suspected data breaches immediately;
- use approved school equipment and consent arrangements for pupil images or recordings;
- ensure any personal online activity does not compromise safeguarding, confidentiality, professional boundaries or the school's reputation; and
- return equipment and school information when requested or when my role ends.

I will not:

- access, create, store or distribute illegal, sexual, hateful, violent or otherwise inappropriate material;
- attempt to bypass filtering/monitoring, use another person's login, disable security controls or install unauthorised software/hardware;
- communicate with pupils through personal social media, messaging, email or gaming accounts;
- enter personal, safeguarding, special-category or confidential data into public or unapproved AI services;
- investigate a safeguarding allegation, conduct an unauthorised device search, or view/copy/forward suspected sexual imagery; or
- make public comments on behalf of the school unless authorised.

I understand that use may be logged and monitored lawfully and proportionately and that misuse may lead to safeguarding, disciplinary, regulatory or criminal action.

Signature: _____ Date: _____

Appendix 4: Staff response pathway

Stage	Required action
1. Protect	Secure immediate safety and medical help. Call 999 for immediate danger or a crime in progress.
2. Listen	Stay calm; take the child seriously; reassure; do not blame or promise confidentiality.
3. Report	Tell the DSL/DDSL directly without delay. Never rely on CPOMS alone for an urgent concern.
4. Record	Make a factual CPOMS entry: exact words, date/time, platform/device, witnesses and action taken.
5. Preserve	Secure devices/messages without investigating. Do not forward harmful content or view/copy sexual imagery.
6. Assess	DSL considers the 4Cs, harm, vulnerability, coercion, reach, continuing contact, possible crime and wider context.
7. Refer/support	DSL decides internal support, Family Help, Children's Social Care, police/CEOP, Prevent or specialist advice.
8. Inform	Parents/carers are normally informed separately unless unsafe or contrary to agency advice.
9. Review	Maintain safety plans; monitor retaliation, rumours, further contact, wellbeing and learning; record outcomes.

Remember

A behaviour response is not a safeguarding assessment. Do not arrange mediation or an apology until the DSL has assessed safety and suitability.

Minimum recording standard

- what was seen, heard or disclosed, separating fact from opinion;
- the child's exact words where possible;
- date, time, place, platform, account/device and how the concern came to light;
- people involved or at risk, including witnesses;
- immediate safety action and any preserved evidence (not sexual imagery);
- who was informed, when and how;
- DSL decision, rationale, referrals, parental contact, support and review date.

Appendix 5: Filtering and monitoring review record

Complete at least annually and whenever a trigger event occurs. Retain the detailed technical record securely and report assurance/actions to the ASC.

Review detail	Record
Date / trigger	
Responsible SLT member	
DSL / DDSL	
IT support representative	
Responsible governor involved	
Systems/providers reviewed	
Networks, locations and device types checked	
Pupil/staff/guest profiles tested	
Current pupil risk profile considered	
SEND/EAL/accessibility considered	
AI, app, image/video/audio and dynamic content coverage considered	
IWF/terrorist/adult-content filtering checks completed	
Monitoring alerts, response times and escalation checked	
Staff reporting knowledge checked	
Temporary exception process checked	
Incidents/trends since last review considered	

Findings and action plan

Finding / gap	Risk	Action / owner	Due / completed

SLT assurance: _____ Date: _____

Governor review/minute reference: _____

Appendix 6: Staff knowledge and training audit

Knowledge / confidence statement	Yes / partly / no and action needed
I can name the DSL/DDSLs and know how to make an urgent report.	
I understand the 4Cs and how online and offline safeguarding overlap.	
I recognise online child-on-child abuse, grooming, exploitation, sextortion and harmful sexual imagery.	
I know not to view, copy, print, save or forward nude/semi-nude imagery.	
I understand my role in supervision, filtering and monitoring and how to report a failure or concern.	
I understand the school's mobile-phone-free expectations.	
I can use approved AI safely and understand privacy, bias, hallucination, copyright and deepfake risks.	
I know the approved communication, data-storage, photography and remote-learning arrangements.	
I can recognise phishing, account compromise, malware and a possible data breach and know whom to tell.	
I know how teaching and reporting are adapted for pupils with SEND or communication needs.	
I understand the adult acceptable use agreement and professional-boundary expectations.	

Name: _____ Role: _____

Training/action agreed: _____

Review date: _____ Manager: _____

Appendix 7: Inky's Staying Safe Online poster

INKY'S SAFE ONLINE ADVENTURE

Be kind • Be careful • Be curious • Tell a trusted adult



Inky's seven smart choices

- Ask before using a new app, site, game or AI tool.
- Keep your name, address, school, location and passwords private.
- Use kind words and respect other people's images and work.
- Remember: people and AI chatbots may not be what they seem.
- Pause and check before you believe, click, buy or share.
- Take healthy breaks and protect sleep, play and family time.
- If anything feels wrong: STOP • CLOSE • TELL.

STOP • CLOSE THE SCREEN • TELL A TRUSTED ADULT

You will not be in trouble for asking for help. Do not reply, pay, meet, forward or keep a worrying image. An adult will help you decide what to do next.

For families: small routines make a big difference

Routine	What it looks like
Talk	Ask what your child enjoys online and make it easy to tell you about mistakes or worries.
Check	Review apps, games, chat, livestreaming, age ratings, location settings and in-app purchases.
Protect	Use parental controls and privacy settings; keep passwords private; update devices.
Balance	Keep younger children's devices in shared spaces and protect sleep, movement and family time.
Report	Save ordinary abusive messages where safe, but never copy sexual imagery. Tell school or police/CEOP as needed.

Appendix 8: Governor assurance checklist

The ASC may use this checklist when approving the policy and receiving the annual online-safety report.

Area	Governor question	Assurance / action
Policy and leadership	Are ownership, delegated oversight and named responsibilities clear, including the SLT and governor leads for filtering and monitoring?	
4Cs and context	Does the school understand current content, contact, conduct and commerce risks for its pupils, including AI-enabled risks?	
Curriculum	Is the National Online Safety/The National College programme taught progressively across the eight areas and reinforced through Computing, PSHE/RSHE and wider learning?	
Inclusion	How is teaching, reporting and support adapted for pupils with SEND, EAL or other vulnerabilities?	
Filtering/monitoring	Has the annual review been completed by SLT with DSL, IT and governor involvement, with device/location checks and actions recorded?	
Mobile phones	Is the school mobile-phone-free throughout the school day, with narrowly defined individual exceptions?	
AI	Are approved use, risk assessment, data protection, copyright, accuracy and harmful-use controls clear?	
Training	Do staff understand online risks, professional conduct, incident response and their filtering/monitoring responsibilities?	
Incidents and voice	What do safeguarding records, pupil voice, parent feedback and behaviour patterns show, and what changed as a result?	
Assurance	Are outstanding actions, owners, deadlines and follow-up reporting clearly recorded?	

Governor decision record

Decision: Approved / Approved subject to amendments / Deferred

Amendments or actions required: _____

Minute reference: _____ Date: _____

Next scheduled review: September 2027 (or sooner if required).