New Direction School

Online Safety and Internet use Policy

Reviewed Date:	Reviewed By:	List of changes	Next Review
August 2021	Luke Collins	• Mobile phones section expanded to include use of mobile phones in school • Social media appendix added.	August 2022
February 2022	Luke Collins	• Reviewed by Luke Collins with some minor grammatical changes made.	January 2023
February 2023	Luke Collins	• Reviewed by Luke Collins with no changes made	February 2024
August 2025	Luke Collins	Redrafted to strengthen filtering and monitoring evidence, governance wording, CPOMS recording, AI, BYOD/personal devices, curriculum links and statutory guidance references.	August 2026

Contents

1. STATEMENT OF INTENT	4
2. LEGAL FRAMEWORK AND LINKED POLICIES	4
3. DEFINITIONS AND CATEGORIES OF ONLINE RISK	5
4. ROLES AND RESPONSIBILITIES	5
5. MANAGING ONLINE SAFETY CONCERNS	7
6. CYBERBULLYING	8
7. CHILD-ON-CHILD SEXUAL ABUSE AND HARASSMENT ONLINE	8
8. GROOMING, EXPLOITATION AND RADICALISATION	9
9. MENTAL HEALTH, HARMFUL ONLINE CHALLENGES AND HOAXES	9
10. CYBER-CRIME	10
11. STAFF TRAINING	10
12. ONLINE SAFETY AND THE CURRICULUM	10
13. USE OF TECHNOLOGY IN THE CLASSROOM	11
14. SMART TECHNOLOGY, MOBILE PHONES AND PERSONAL DEVICES	11
15. EDUCATING PARENTS AND CARERS	12
16. INTERNET ACCESS, FILTERING AND MONITORING	12
17. NETWORK SECURITY	14
18. EMAIL AND COMMUNICATION SYSTEMS	14
19. GENERATIVE ARTIFICIAL INTELLIGENCE (AI)	14
20. SOCIAL MEDIA, WEBSITE AND IMAGES	15
21. REMOTE EDUCATION	15
22. INCIDENT RECORDING, EVIDENCE AND INSPECTION READINESS	15
23. MONITORING AND REVIEW	16
APPENDIX 1: FILTERING AND MONITORING REVIEW CHECKLIST	17
APPENDIX 2: ONLINE SAFETY INCIDENT RESPONSE CHECKLIST	17
APPENDIX 3: PUPIL ACCEPTABLE USE SUMMARY	18

1. Statement of intent

New Direction School recognises that the safe and effective use of technology is an important part of raising educational standards, supporting communication, promoting independence, preparing pupils for adulthood and enhancing teaching and learning.

The school is committed to providing a safe online environment for pupils, staff and visitors. Online safety is treated as a safeguarding matter and is embedded across the curriculum, staff training, behaviour expectations, safeguarding procedures, pastoral support and the school's filtering and monitoring arrangements.

This policy sets out how the school will protect pupils and staff when using the internet, digital technology, online platforms, communication systems, mobile devices, smart technology and emerging technologies, including generative artificial intelligence.

The school recognises that technology is a significant component in many safeguarding and wellbeing issues. Online safety will therefore be a running and interrelated theme throughout school policies and practice, including safeguarding, behaviour, anti-bullying, PSHE/RSE, staff conduct, data protection, remote education and curriculum planning.

2. Legal framework and linked policies

This policy has due regard to relevant legislation, statutory guidance and non-statutory guidance including, but not limited to:

- Keeping Children Safe in Education 2025 (KCSIE)
- Working Together to Safeguard Children 2026
- Education Act 2002, including section 157 duties for independent schools
- The Education (Independent School Standards) Regulations 2014, including Part 3 welfare, health and safety of pupils
- The Online Safety Act 2023
- The Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- The Equality Act 2010
- The Prevent duty guidance: England and Wales 2023
- DfE filtering and monitoring standards for schools and colleges
- DfE Meeting digital and technology standards in schools and colleges
- DfE Teaching online safety in schools
- DfE Searching, screening and confiscation guidance
- DfE Generative artificial intelligence in education guidance
- DfE Generative AI product safety standards
- UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people
- UKCIS Education for a Connected World
- National Cyber Security Centre Small Business Guide: Cyber Security

This policy should be read alongside the following New Direction School policies and procedures:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy

- Anti-Bullying Policy
- Data Protection Policy
- Staff ICT and Electronic Devices Policy
- Remote Education Policy
- Disciplinary Policy and Procedure

3. Definitions and categories of online risk

For the purposes of this policy, online safety means safeguarding children, young people and adults when they use technology and when they are affected by technology use, whether this occurs on site, off site, during the school day or outside school hours.

Online safety risks are considered under four broad categories:

Content: being exposed to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, discrimination, radicalisation, extremism, misinformation, disinformation, fake news and conspiracy theories.

Contact: being subjected to harmful online interaction with other users, including peer pressure, commercial exploitation, grooming, adults posing as children, exploitation for sexual, criminal or financial purposes and unsafe contact from unknown individuals.

Conduct: online behaviour that increases the likelihood of harm to self or others, including bullying, harassment, abuse, sharing explicit images, sharing pornography, sexual comments, online abuse in relationships, impersonation, doxxing or encouraging harmful behaviour.

Commerce: risks such as online gambling, inappropriate advertising, phishing, scams, fraud, in-app purchases, financial exploitation and other forms of online commercial harm.

4. Roles and responsibilities

4.1 Proprietor and Directors

The Proprietor and Directors are responsible for ensuring that this policy is effective, implemented and compliant with relevant legislation and statutory guidance. They will:

- ensure arrangements are in place to safeguard and promote the welfare of pupils, including online safety arrangements;
- ensure the DSL's remit includes online safety, filtering and monitoring;
- ensure appropriate filtering and monitoring systems are in place and reviewed at least annually;
- receive assurance that filtering and monitoring roles, responsibilities, checks and escalation routes are clear and effective;
- ensure staff receive safeguarding and child protection training, including online safety, at induction and at regular intervals;
- ensure online safety is considered in curriculum planning, staff conduct, data protection, behaviour, anti-bullying, Prevent and remote education arrangements;
- ensure this policy is reviewed annually and following significant incidents or statutory guidance changes.

4.2 Head of Education / DSL

Luke Collins, as Head of Education and Designated Safeguarding Lead, has lead responsibility for online safety. The Head of Education/DSL will:

- take lead responsibility for safeguarding and child protection concerns arising from online activity;
- ensure online safety is a running and interrelated theme across school policies and practice;
- ensure staff know how to report online safety concerns, including filtering and monitoring alerts;
- ensure online safety concerns, disclosures, filtering/monitoring alerts and actions are recorded on CPOMS;
- liaise with children's social care, the police, Derbyshire safeguarding arrangements and other local authorities where appropriate, including Nottinghamshire, Rotherham and Sheffield;
- ensure online safety is included in safeguarding induction, regular safeguarding updates and whole-school training;
- work with Tel-Group to review filtering and monitoring reports, checks, incidents and technical arrangements;
- ensure filtering and monitoring is reviewed annually and after significant incidents, technology changes or changes in pupil risk profile;
- ensure pupils with SEND, vulnerabilities or contextual risks receive appropriate online safety support;
- organise appropriate parent/carer engagement on online safety issues.

4.3 Deputy DSLs

The Deputy DSLs are Hannah Oliver, Emily Smith and Nikki Morris. They will support the DSL by responding to online safety concerns, recording actions on CPOMS, supporting pupils and staff, and escalating concerns in line with the Child Protection and Safeguarding Policy.

4.4 ICT technical support

Tel-Group provides ICT technical support. Tel-Group will work with the Head of Education/DSL and the Proprietor/Directors to:

- implement and maintain appropriate filtering, monitoring, security and access controls;
- support technical checks of filtering and monitoring systems;
- provide reports and technical information to support safeguarding oversight;
- investigate technical concerns, attempted breaches, malware, phishing and network security incidents;
- support risk assessments for new systems, platforms, devices, apps and AI tools;
- maintain appropriate technical security arrangements including firewalls, antivirus, updates, account security and access controls.

4.5 All staff

All staff are responsible for safeguarding pupils online and modelling safe and professional use of technology. Staff will:

- read and follow this policy, the Staff Code of Conduct, safeguarding procedures and relevant acceptable use agreements;
- report online safety concerns immediately to the DSL or a Deputy DSL;
- record concerns on CPOMS in line with school procedure;

- never promise confidentiality where a safeguarding concern is disclosed;
- maintain professional boundaries in all online communication;
- use school systems and personal devices only as permitted by school policy;
- actively supervise pupils when technology is used in lessons or activities;
- challenge unsafe, unkind, discriminatory or harmful online behaviour;
- teach or reinforce online safety where relevant to their role.

4.6 Pupils

Pupils are expected to use technology safely, responsibly and respectfully. Pupils will be supported to:

- follow the pupil acceptable use agreement and school rules for technology and mobile devices;
- tell a trusted adult if they see or experience anything online that worries, upsets or harms them;
- understand that online behaviour has real-world consequences;
- respect the privacy, dignity and rights of others;
- avoid sharing personal information, images, passwords or contact details in unsafe ways;
- understand how to report and block harmful content or contact where appropriate.

5. Managing online safety concerns

All online safety concerns will be treated as safeguarding concerns unless it is clear that they are not safeguarding related. Concerns may arise from pupil disclosures, staff observations, curriculum discussions, parent/carer reports, filtering or monitoring alerts, peer reports, online behaviour, emails, device use, social media, AI tools or external information.

Staff must report concerns to the DSL or a Deputy DSL without delay. Where there is an immediate risk of harm, staff must act immediately in line with the Child Protection and Safeguarding Policy, including contacting emergency services if necessary.

Online safety concerns will be recorded on CPOMS. Records will include the nature of the concern, pupils involved, actions taken, referrals made, parent/carer contact where appropriate, decisions made, and any follow-up support or monitoring.

The DSL will decide the appropriate response, which may include:

- speaking with the pupil and providing support;
- contacting parents/carers where safe and appropriate;
- preserving evidence without forwarding, copying or sharing harmful sexual images;
- liaising with Tel-Group to review filtering or monitoring information;
- making a referral to children's social care;
- contacting the police where there is suspected illegal activity or immediate risk;
- seeking advice from the local authority, safeguarding partnership, UK Safer Internet Centre, CEOP, IWF or other relevant agencies;
- taking action under the Behaviour Policy, Anti-Bullying Policy or Child-on-Child Abuse Policy;
- reviewing risk assessments, supervision, curriculum input, filtering and monitoring settings or device access.

The school will avoid unnecessarily criminalising pupils where behaviour may have arisen through ignorance, developmental curiosity or a safeguarding need. However,

the school will always prioritise the safety and welfare of pupils and will seek advice from statutory agencies where needed.

6. Cyberbullying

Cyberbullying is bullying that takes place using technology. It may include threatening, intimidating, humiliating, discriminatory or harmful messages, posts, images, videos, calls, emails, group chats or social media activity.

Cyberbullying may include:

- abusive or threatening messages;
- sharing embarrassing or harmful images or video clips;
- impersonation or using another person's account;
- excluding, humiliating or targeting a pupil in group chats;
- posting defamatory or discriminatory content;
- online abuse linked to protected characteristics, including racism, misogyny, homophobia, biphobia, transphobia, disability-related abuse or religious discrimination;
- abuse between young people in intimate relationships.

The school will not tolerate cyberbullying of pupils, staff or other members of the school community. Incidents will be managed in line with the Anti-Bullying Policy, Behaviour Policy, Child Protection and Safeguarding Policy and Staff Code of Conduct as appropriate.

The school recognises that pupils with SEND, pupils who are care experienced, LGBTQ+ pupils, pupils with mental health needs and pupils experiencing wider vulnerability may be at increased risk of online abuse or bullying. Support and response will be tailored accordingly.

7. Child-on-child sexual abuse and harassment online

Pupils may use technology as a vehicle for sexual abuse, sexual harassment, coercion, intimidation or harmful sexual behaviour. This may occur on or off school premises, during or outside the school day, and may involve school or personal devices.

Examples include:

- sexualised bullying, jokes, taunts or comments;
- unwanted sexual messages, images, videos or calls;
- pressuring someone to share images or engage in sexual activity online;
- consensual or non-consensual sharing of nudes or semi-nudes;
- upskirting or image-based abuse;
- threatening to share sexual images or information;
- abuse between young people in intimate relationships;
- using social media or messaging platforms to continue harassment after an incident is reported.

All staff will maintain a zero-tolerance approach to sexual harassment and sexual violence. Behaviour will never be dismissed as "banter", "having a laugh", "part of growing up" or "boys being boys".

Staff will be aware that creating, possessing or distributing indecent images of children under 18 is a criminal offence, even where the image was created by the child themselves or shared with consent. Staff must not view, copy, print, forward or share sexual images of children unless there is an unavoidable and clear safeguarding reason to do so, in line with national guidance.

Concerns will be reported to the DSL and managed in line with the Child Protection and Safeguarding Policy and Child-on-Child Abuse Policy. The DSL will consider the wishes and feelings of the child, immediate safety, wider risks to other pupils, evidence preservation, parent/carer involvement, referrals and support for both the child who has been harmed and the child alleged to have caused harm.

8. Grooming, exploitation and radicalisation

8.1 Grooming and exploitation

Grooming is a process in which an adult or another child builds trust, emotional connection or control with a child in order to manipulate, exploit or abuse them. Grooming can take place online, offline or both.

Staff will be alert to signs that a pupil may be experiencing online grooming or exploitation, including secrecy about online activity, unexplained gifts or money, relationships with unknown or older individuals, changes in behaviour, fearfulness, sexualised behaviour, missing episodes, new devices, or reluctance to discuss online contacts.

Online exploitation may include child sexual exploitation, child criminal exploitation, coercion into sharing images, forced involvement in scams, drug supply, county lines activity, extremist networks or other forms of harm. The school will use the term child sexual abuse material or indecent images of children, rather than outdated terminology.

8.2 Radicalisation and extremism

The school recognises that pupils may be exposed to extremist content, terrorist material, conspiracy theories, hateful narratives or grooming by individuals or groups online. Filtering and monitoring, staff vigilance, Prevent training, curriculum education and safeguarding procedures will all contribute to the school's approach to reducing this risk.

Concerns about radicalisation will be reported to the DSL immediately and managed in line with the Prevent Duty Policy and Child Protection and Safeguarding Policy. The DSL will seek advice or make a referral to Channel or other appropriate agencies where necessary.

9. Mental health, harmful online challenges and hoaxes

The school recognises that online activity can affect pupils' mental health positively and negatively. Risks include harmful content relating to self-harm, suicide, eating disorders, body image, bullying, isolation, sleep disruption, addictive behaviours, hate content and comparison culture.

Concerns about the impact of online activity on a pupil's mental health will be recorded and managed in line with safeguarding procedures and the school's wider SEMH support arrangements.

An online hoax is a deliberate falsehood designed to appear truthful and to cause fear, distress or confusion. A harmful online challenge is an online trend that may place pupils at risk of physical, emotional, social, sexual or reputational harm.

Where staff become aware of a harmful online challenge or hoax, they will report it to the DSL. The DSL and Head of Education will assess the scale, credibility and nature of the risk before responding. Responses will be proportionate and will avoid unnecessarily increasing pupil exposure to the harmful content.

The school may seek advice from reliable sources such as the UK Safer Internet Centre, local safeguarding partners, the police, the local authority or other trusted agencies.

10. Cyber-crime

Cyber-crime is criminal activity committed using computers or the internet. It may be cyber-enabled, such as fraud, exploitation or drug supply arranged online, or cyber-dependent, such as hacking, malware, denial-of-service attacks or obtaining tools designed to compromise systems.

The school recognises that some pupils may have strong digital skills and may be vulnerable to becoming involved in cyber-crime deliberately or inadvertently. Concerns will be reported to the DSL, who may consider support, safeguarding intervention or a referral to Cyber Choices where appropriate.

Pupils will be taught to use technology safely, responsibly and lawfully, including understanding the legal and personal consequences of hacking, accessing systems without permission, sharing passwords, using malware or participating in online fraud.

11. Staff training

All staff will receive online safety training as part of induction and ongoing safeguarding training. Training will include:

- how technology can facilitate abuse, exploitation, grooming, bullying, harassment and radicalisation;
- the four categories of online risk: content, contact, conduct and commerce;
- how to respond to disclosures and report concerns;
- how to record concerns on CPOMS;
- staff responsibilities in relation to filtering and monitoring;
- safe and professional use of technology, communication systems and social media;
- AI risks, data protection and appropriate use;
- harmful online narratives including misinformation, disinformation and conspiracy theories;
- the needs of vulnerable pupils, including pupils with SEND.

The DSL will ensure staff receive updates when online safety risks, local concerns, technology use or statutory guidance changes.

12. Online safety and the curriculum

Online safety will be embedded across the curriculum and particularly through PSHE, PSE, Independence, ASDAN PSE, tutor time, Zones of Regulation, employability and wider pastoral work. Teaching will be age-appropriate, developmentally appropriate and adapted for pupils with SEND and additional vulnerabilities.

Pupils will be taught the knowledge, skills and behaviours needed to navigate online spaces safely and confidently, including:

- how to evaluate what they see online;
- how to recognise persuasion, manipulation, misinformation and disinformation;
- how to identify trusted sources and fact-check information;
- how to manage privacy, personal information and digital reputation;
- acceptable and unacceptable online behaviour;
- how to report, block and seek support;
- the law and consequences around online sexual images, harassment, cyberbullying, hacking and harmful content;
- how to recognise unsafe contact, grooming, exploitation and pressure;
- how to understand commercial risks, scams, phishing, gambling and financial exploitation;
- safe, responsible and ethical use of AI and emerging technologies.

The DSL will be involved in planning and reviewing online safety education. Pupils may be consulted, where appropriate, because they may have insight into current platforms, trends and risks.

Staff will review external resources before using them to ensure they are accurate, age appropriate, accessible and suitable for the needs of the cohort. External visitors may be used where appropriate and will be agreed by the Head of Education/DSL.

Before teaching sensitive online safety content, staff will consider whether pupils may have lived experience of the issue. Lessons will be planned to avoid identifying or exposing pupils and to maintain a safe, respectful learning environment. Safeguarding concerns arising from lessons will be reported to the DSL.

13. Use of technology in the classroom

Technology used in lessons may include computers, laptops, tablets, intranet resources, email, cameras, online platforms, accessibility tools and approved educational apps.

Before using websites, apps, online tools, AI products or digital platforms with pupils, staff must consider whether they are suitable, safe, age appropriate, accessible and compliant with data protection expectations. Staff must not require pupils to use platforms that have not been approved or risk assessed where approval is required.

Staff supervising pupils using technology must actively monitor use through appropriate classroom supervision. This includes positioning themselves to view screens where practical, checking pupils remain on approved sites or platforms, challenging unsafe behaviour, and reporting concerns to the DSL.

Pupils will be supervised when using online materials. The level of supervision will reflect pupils' age, ability, SEND, vulnerability, task, device and online risk.

14. Smart technology, mobile phones and personal devices

Pupils are not permitted to use personal mobile phones, smart watches, smart devices or other personal technology during the school day. These must be handed in on arrival in line with school procedures. Exceptions may only be made by the Head of Education/DSL for an agreed medical, safeguarding or accessibility reason, and must be risk assessed.

The school recognises that personal devices may provide unrestricted access to mobile networks. Pupils must not use 3G, 4G, 5G or other mobile data connections to bypass school filtering or monitoring arrangements.

Staff may use school devices provided to them or their own devices logged onto the staff Wi-Fi network, where this is permitted by the Staff ICT and Electronic Devices Policy and Data Protection Policy. Staff personal devices used for work purposes must be secure, password protected and used only in a way that maintains confidentiality, professionalism and safeguarding expectations.

Personal devices must not be used to store pupil photographs, safeguarding information, confidential pupil information or school records unless expressly authorised and securely managed. Staff must not use personal accounts or personal messaging services to communicate with pupils.

Any personal device connected to the school network will be subject to appropriate filtering and monitoring controls where technically possible. Use of personal devices on school systems may be withdrawn where there are safeguarding, conduct, security or data protection concerns.

15. Educating parents and carers

The school will work in partnership with parents and carers to support pupils to stay safe online at school and at home. Parents and carers will be provided with information about online safety risks and the school's expectations.

Parent/carer information may include guidance on:

- parental controls and home filtering;
- age ratings and privacy settings;
- cyberbullying and online harassment;
- grooming, exploitation and unsafe contact;
- nudes and semi-nudes;
- harmful content linked to self-harm, suicide, eating disorders, misogyny, pornography, extremism or hate;
- gaming, gambling, scams and in-app purchases;
- safe use of social media, messaging apps and AI tools;
- how to report concerns to school or external agencies.

Information may be shared through newsletters, meetings, direct contact, online resources, the school website and pastoral communication.

16. Internet access, filtering and monitoring

All members of the school community are expected to use the school's internet network for school work rather than mobile data networks, because the school network has appropriate filtering and monitoring arrangements.

16.1 Filtering

The school will maintain appropriate filtering to protect pupils from illegal, inappropriate and harmful content while avoiding unreasonable over-blocking that would restrict teaching, learning or safeguarding education.

The school will seek assurance from its filtering provider that, as a minimum, filtering blocks access to known child sexual abuse material, unlawful terrorist content and adult content, using recognised lists and services where applicable, such as the Internet Watch Foundation and Counter Terrorism Internet Referral Unit lists. Safe search will be enabled and locked where technically possible on school-managed devices and browsers.

16.2 Monitoring

The school will maintain appropriate monitoring arrangements for school networks and school-owned devices. Monitoring may include automated alerts, usage reports, audit logs, keyword alerts, safeguarding reports or other appropriate technical methods.

Monitoring alerts and concerns will be escalated to the DSL or Deputy DSLs. High-risk concerns, including suspected illegal activity, sexual harm, self-harm, suicide, radicalisation, exploitation or serious bullying, will be escalated without delay.

16.3 Roles, checks and records

The DSL and Head of Education will hold safeguarding oversight of filtering and monitoring. Tel-Group will provide technical implementation and support. The Proprietor and Directors will seek assurance that arrangements are suitable and effective.

The school will keep records of filtering and monitoring checks, annual reviews, significant alerts, changes to filtering settings, blocked or allowed website decisions, risk assessments, actions taken and escalation decisions. These records will be available for safeguarding audit and inspection.

Filtering and monitoring checks will include, where relevant:

- school networks and Wi-Fi;
- school-owned devices;
- staff work devices;
- guest or visitor access;
- school-managed devices used off site;
- staff personal devices connected to the staff Wi-Fi network;
- approved online platforms, apps and AI tools;
- changes to systems, devices, software or internet provision.

16.4 Review

Filtering and monitoring arrangements will be reviewed at least annually and following any significant safeguarding incident, technology change, system change, change to pupil risk profile, new device deployment, remote learning arrangement, BYOD change or new online platform.

The annual review will consider the needs and risk profile of pupils, including SEND and vulnerability; what is blocked and allowed; monitoring reports; safeguarding incidents; pupil and staff feedback; PSHE/RSE curriculum needs; technical limitations;

off-site use; AI tools; mobile data risks; and whether staff understand their responsibilities.

16.5 Breaches and illegal content

Deliberate attempts to bypass filtering or monitoring will be reported to the DSL and managed in line with the Behaviour Policy, Staff Code of Conduct, Disciplinary Policy or safeguarding procedures as appropriate.

If material believed to be illegal is accessed, whether deliberately or accidentally, the school will act immediately. The DSL or Head of Education will seek appropriate advice and may report to the police, CEOP, IWF or other relevant agencies. Staff must not unnecessarily view, copy, save, print or forward illegal or harmful material.

17. Network security

The school will maintain appropriate technical security arrangements, including firewalls, antivirus or endpoint protection, system updates, access controls, password procedures and account management.

Users must not share passwords or login details with anyone. Users must lock devices and systems when not in use. Staff and pupils must not download unapproved software, open suspicious attachments or click unknown links. Suspected malware, phishing, unauthorised access or cyber-attacks must be reported to Tel-Group and the DSL/Head of Education.

Cyber incidents will be managed in line with the Cyber-security Policy and Cyber Response and Recovery Plan. Where a cyber incident creates a safeguarding or data protection risk, the DSL and DPO will be involved.

18. Email and communication systems

Email and school communication systems will be used in line with the Data Protection Policy, Confidentiality Policy, Acceptable Use Agreement and Staff Code of Conduct.

Staff and pupils may only use approved school accounts for school-related work. Personal email accounts must not be used for school business or pupil communication. Sensitive or personal information must be shared securely and only where there is a lawful basis and need to know.

Users must report suspicious emails, phishing attempts, malware, inappropriate links, abusive communication or data breaches. Chain emails, spam and messages from unknown sources should not be opened and should be deleted or reported as appropriate.

19. Generative artificial intelligence (AI)

The school recognises that generative AI and emerging technologies can offer educational and workload benefits, but may also present safeguarding, data protection, bias, misinformation, intellectual property, plagiarism, age restriction and harmful content risks.

AI tools may only be used where the benefits outweigh the risks and where appropriate safeguards are in place. Pupils may only use generative AI in school with

staff approval, appropriate supervision and age-appropriate tools with suitable safety features.

The school will:

- comply with age restrictions and terms of use for AI tools;
- risk assess AI tools before pupil use where appropriate;
- ensure staff and pupils do not enter personal, sensitive, safeguarding or confidential data into AI tools unless there is an approved lawful basis and secure arrangement;
- consider bias, accuracy and misinformation risks when using AI outputs;
- ensure AI does not replace professional judgement, safeguarding decision-making or teacher assessment without appropriate oversight;
- include safe and ethical use of AI in online safety education;
- follow the school's Safe Use of AI Policy.

20. Social media, website and images

20.1 Social media

Staff and pupils must follow the school's Social Media Policy. Staff must maintain professional boundaries online and must not communicate with pupils through personal social media accounts, personal messaging apps or personal gaming accounts.

Concerns about social media content involving pupils, staff, parents/carers or the school will be assessed by the DSL/Head of Education and managed in line with safeguarding, behaviour, anti-bullying, disciplinary or communication procedures as appropriate.

20.2 Website

The Head of Education is responsible for ensuring the school website is appropriate, accurate, up to date and compliant with statutory publication expectations where applicable. Online content must protect pupils' privacy and dignity.

20.3 Photographs and images

Images of pupils will be taken, stored and used in line with the Photography and Images Policy and Data Protection Policy. Staff must not use personal devices to take or store pupil images unless expressly authorised in exceptional circumstances and managed securely.

21. Remote education

Remote education will be delivered in line with the Remote Education Policy. Online safety expectations apply during remote learning, including professional conduct, pupil supervision, appropriate communication, camera use, safeguarding reporting, data protection, platform safety and access to support.

Where pupils use school-managed devices off site, filtering and monitoring will apply where technically possible. Where this is not technically possible, the school will risk assess use and apply alternative safeguards, such as restricted access, supervision, device settings, parental engagement or withdrawal of access.

22. Incident recording, evidence and inspection readiness

The school will retain evidence that this policy is implemented effectively. Evidence may include:

- CPOMS records of online safety concerns, actions and outcomes;
- filtering and monitoring annual review records;
- routine filtering and monitoring check records;
- records of blocked/allowed website decisions and reasons;
- monitoring alerts and response records;
- staff safeguarding and online safety training records;
- pupil online safety curriculum coverage;
- pupil acceptable use agreements;
- parent/carer communications and online safety resources;
- risk assessments for devices, apps, online platforms, AI tools or remote learning;
- records of cyber incidents and response actions;
- policy review records and proprietor/director oversight.

Evidence will be stored securely and in accordance with the Data Protection Policy and records management expectations.

23. Monitoring and review

This policy will be reviewed annually by the Head of Education/DSL and approved by the Proprietor and Directors. It will also be reviewed following significant online safety incidents, safeguarding concerns, filtering or monitoring changes, cyber incidents, new technology use, AI developments or updates to relevant statutory guidance.

The school will ensure that staff, pupils, parents/carers and relevant visitors are made aware of this policy in an appropriate and accessible way. Parents/carers may request a paper copy from the school office.

Appendix 1: Filtering and monitoring review checklist

This checklist should be used to evidence annual and event-driven reviews of filtering and monitoring arrangements.

Area	Review prompt	Evidence / action required
Roles and responsibilities	Are safeguarding, technical and proprietor/director responsibilities clearly assigned?	Record named leads and date reviewed.
Filtering coverage	Does filtering apply to networks, Wi-Fi, school-owned devices and off-site devices where possible?	Record systems checked and any gaps.
Illegal and harmful content	Are illegal child sexual abuse material, unlawful terrorist content and adult content blocked as a minimum?	Record provider assurance and test/check evidence.
Safe search	Is safe search enabled and locked where technically possible?	Record checks and exceptions.
Monitoring alerts	Are monitoring reports or alerts reviewed by appropriate staff?	Record frequency, reviewer and escalation route.
Over-blocking	Are blocked sites preventing reasonable teaching, learning or safeguarding education?	Record allowed/blocked decisions and risk assessment.
Pupil risk profile	Have SEND, vulnerability, age, curriculum and contextual risks been considered?	Record considerations and adaptations.
Staff knowledge	Do staff know how to report concerns and what their role is?	Record training and updates.
AI and emerging tech	Have AI tools and new platforms been considered?	Record approved tools and risk assessments.
Incident learning	Have incidents, alerts and concerns informed changes?	Record lessons learned and actions.

Appendix 2: Online safety incident response checklist

- Ensure the immediate safety of the pupil or pupils involved.
- Report the concern to the DSL or Deputy DSL without delay.

- Record the concern on CPOMS, including context, actions and decisions.
- Do not view, copy, save, print, forward or share sexual or illegal content unless unavoidable for safeguarding reasons.
- Preserve evidence safely where appropriate, for example URLs, usernames, dates, times or screenshots taken by the DSL where lawful and necessary.
- Consider whether parents/carers should be informed, unless doing so would increase risk.
- Consider whether children's social care, police, CEOP, IWF, Prevent/Channel or another agency should be contacted.
- Consider support for the pupil harmed, the pupil alleged to have caused harm and any wider peer group affected.
- Consider behaviour, anti-bullying, child-on-child abuse, staff conduct or disciplinary procedures if relevant.
- Review whether filtering, monitoring, supervision, curriculum content, device access or risk assessments need to be changed.

Appendix 3: Pupil acceptable use summary

Pupils will be taught and reminded of the following age-appropriate expectations:

- I will use school technology safely, respectfully and only for learning or agreed activities.
- I will not try to access harmful, illegal or inappropriate content.
- I will not use mobile data or other methods to bypass school filtering or monitoring.
- I will not share my password or use someone else's login.
- I will not send unkind, threatening, bullying, sexual, discriminatory or harmful messages or images.
- I will not take, send, ask for or share nudes or semi-nudes.
- I will tell a trusted adult if I see something online that worries, upsets or harms me.
- I will tell staff if someone contacts me online in a way that feels unsafe or makes me uncomfortable.
- I will not share personal information, images or contact details in unsafe ways.
- I understand that the school may monitor use of school systems and devices to help keep everyone safe.