Online Safety Policy

Policy Author	Mr K Hopkins	Date of Approval	28.09.26
Policy Approval	Full Governing Board	Next Review Date	September 2027

Statement of intent

Oldbrook First School and Nursery understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

This policy applies to staff, governors, volunteers, contractors and visitors, alongside age-appropriate pupil expectations. It covers online harm on or off site, including personal devices where the conduct affects pupils, professional duties or school information. Read with the updated Internet and Acceptable Use Policy and Low Level Concerns Policy.

Legal framework

This policy applies the legislation and statutory guidance below, as amended, and the current supporting guidance linked in the Sources section. Statutory safeguarding duties remain with the school. DfE digital standards and AI guidance describe recommended practice; platform duties under the Online Safety Act do not replace school safeguarding responsibilities.

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 and UK GDPR as amended, including relevant commenced provisions of the Data (Use and Access) Act 2025.
- DfE filtering and monitoring core standard and cyber security core standard, current September 2026 editions. [3, 4]
- DfE (2021) 'Harmful online challenges and online hoaxes'

- Keeping children safe in education 2026 and Working together to safeguard children 2026, both statutory guidance. [1, 2]
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE generative artificial intelligence in education guidance and generative AI product safety standards. [5]
- UKCIS Sharing nudes and semi-nudes advice for education settings, updated March 2024, including AI-generated imagery. [8]
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- Current NCSC advice and the DfE cyber security core standard
- September 2026 EYFS framework and screen-use guidance
- Mobile phones in schools statutory guidance
- Revised relationships and health education guidance effective from 1 September 2026. [4, 6, 7, 9]

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Staff Device Agreement
- Prevent Duty Policy
- Remote Education Policy

Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the designated safeguarding lead's (DSL) remit covers online safety, with deputy cover and sufficient time, authority, training and resources.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff receive safeguarding and online safety training at induction, regular training and updates at least annually. All staff must read KCSIE 2026 Part one in full; a summary is not a substitute. [1]
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Seeking assurance against the DfE filtering, monitoring and cyber security standards, identifying a responsible governor and senior leader, and ensuring gaps, actions, owners and deadlines are recorded. [3, 4]

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technician to conduct termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.
- Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.
- Appointing an SLT digital lead in line with the Cyber-security Policy.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Maintaining safeguarding expertise through DSL training at least every two years and knowledge updates at least annually, including online risks and additional needs of pupils with SEND. [1]
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technician.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Maintaining accessible reporting routes for staff, children and parents, including deputy cover and arrangements outside school hours. Ensuring safeguarding alerts are reviewed promptly and do not wait for a termly technical check.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and ICT technician to conduct termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

ICT technician will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Maintaining secure technical controls, providing reports and promptly escalating safeguarding alerts to the DSL or deputy. Technical staff support the response but do not determine safeguarding outcomes.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct termly light-touch reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting safeguarding concerns immediately to the DSL or deputy, cyber incidents to ICT and the Headteacher, and suspected personal-data breaches to the DPO. Adult-conduct concerns follow the separate routes below.

- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Learning and following age-appropriate acceptable-use rules with adult support and reasonable adjustments. Pupils are not responsible for making the school's systems safe.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online
- All computing lessons contain an element of online safety teaching

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

Listen to the child, take their wishes seriously and explain next steps in an age-appropriate way. Do not promise secrecy. The DSL will assess risk to the child and others and involve children's social care or police where required. Involve parents unless doing so would increase risk, compromise an investigation or conflict with agency advice; record the decision and support offered. [1, 2]

Share necessary and proportionate safeguarding information securely on an appropriate lawful basis, recording decisions and reasons. Consent is not always required and uncertainty must not delay protection. Explain sharing where safe to do so. Follow the school's safeguarding and data-protection procedures, including the information-sharing commencement note below. [2, 11]

Report concerns about an adult's online conduct to the Headteacher immediately, or to the Chair of Governors if about the Headteacher. Apply KCSIE Part four, the allegations procedure and Low Level Concerns Policy. Consult the LADO if the harm threshold may be met or classification is uncertain. Use direct safeguarding or whistleblowing routes where a conflict prevents safe reporting. [1]

The DSL will assess pupil concerns, protect those affected and coordinate with relevant staff and agencies. Do not undertake an internal investigation that could compromise police or social-care enquiries. Safeguarding support and any proportionate behavioural response must be considered separately.

Where a child is in immediate danger call 999. Make an immediate social-care and/or police referral where a child is suffering or likely to suffer harm. Any staff member may make a referral where necessary; absence of the Headteacher or DSL must not delay action. Inform the DSL as soon as possible. [1, 2]

Avoid unnecessarily criminalising children, but do not use this principle to delay a required referral. The DSL follows KCSIE and UKCIS criteria, seeking police or social-care advice where uncertain, particularly where an adult, coercion, exploitation, threats or a very young child is involved. [1, 8]

Record concerns, the child's account, actions, referrals, decisions and reasons promptly in the restricted safeguarding record. Record dates, relevant usernames or web addresses without copying suspected illegal images. The DSL reviews outcomes and recurring patterns and arranges ongoing support.

Immediate response to images and sexual extortion

Do not intentionally view, copy, save, print, screenshot, forward or ask anyone to send suspected sexual imagery of a child, including AI-generated images. Do not ask a child to show the image or direct deletion before the DSL considers evidence and police advice. Secure the device as directed without exploring its contents. Only the DSL may consider exceptional viewing under the UKCIS criteria, recording the justification. [8]

The DSL must follow UKCIS referral criteria, including adult involvement, coercion or blackmail, sexual acts involving a child under 13, concern about capacity to consent or immediate risk. Seek advice if uncertain. For sexual extortion, reassure the child they are not to blame, do not pay or comply with demands, and obtain police advice promptly. Support safe reporting and removal through appropriate services without circulating the material. [8]

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as lesbian, gay, bisexual, or gender questioning pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting: taking an image beneath a person's clothing without consent or reasonable belief in consent, to observe their genitals or buttocks (or underwear covering them) for sexual gratification or to cause humiliation, distress or alarm. Report suspected image-based abuse even if staff are unsure of its precise legal classification.
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Sharing nude, semi-nude or sexualised images, including altered or AI-generated images, with or without permission; threats to share images and financially motivated sexual extortion.
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Indecent photographs or pseudo-photographs of a person under 18 can be illegal to create, possess or distribute, including self-generated and AI-created material. A child's agreement does not make such material lawful. Staff must follow the image-incident procedure below rather than viewing or forwarding it to establish whether an offence has occurred. [8]

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy, Child Protection and Safeguarding Policy, and the Social Media Policy.

Respond to online child-on-child abuse wherever it occurs, including on personal devices and outside school. Refer immediately to the DSL for safeguarding assessment, support and appropriate agency involvement. Do not dismiss an incident as banter, ordinary curiosity or less serious because it is online.

Grooming and exploitation

Grooming involves building trust, a relationship or emotional connection to manipulate, exploit or abuse a child. It can be undertaken by adults or other children, online or offline, and may involve impersonation, gifts, threats or pressure.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

CSE can occur online without physical contact, including coercion into sexual activity, requests for imagery, live-streamed abuse and sexual extortion. Use the term child sexual abuse material, not "child pornography"; children cannot be responsible for their own exploitation. Refer concerns promptly even without a disclosure.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the school's Child Protection and Safeguarding Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "**online hoax**" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "**harmful online challenges**" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Cyber incidents and personal data breaches

Report cyber incidents immediately to ICT and the Headteacher, and personal-data incidents to the DPO; alert the DSL if a child may be at risk. Follow the response plan, preserve logs and evidence safely, and do not wipe devices or attempt improvised recovery. Maintain protected backups, tested restoration and continuity arrangements for safeguarding and school operations. [4]

Record all personal-data breaches and the risk assessment. Notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to risk individuals' rights and freedoms. Notify affected people without undue delay where the high-risk threshold is met. Do not delay a required initial report until the investigation is complete. [10]

Online safety training for staff

Staff training includes online abuse and exploitation, reporting, safe handling of imagery, filtering and monitoring responsibilities, AI risks and the needs of vulnerable pupils. Training is provided on induction and updates at least annually. All staff read KCSIE 2026 Part one in full. [1]

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

Online safety and the curriculum

Online safety is taught through the subjects below and the school's sequenced curriculum in Appendix 1. From 1 September 2026, planning has regard to the revised statutory relationships and health education guidance. [9]

- Relationships and health education
- PSHE
- Computing and Online Safety

Teaching is matched to pupils' age, development and SEND. Staff awareness of serious harms does not mean every harm is taught explicitly to every age group. Staff use safe, concrete examples, support disclosure and never show harmful material to demonstrate a risk.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks

For nursery, Reception and Years 1–2, teach that online information and pictures may be untrue or upsetting, that children can stop and seek help, and that a trusted adult can help check information. Plan any sensitive content under the relationships and health education guidance and the DSL's advice; do not deliver graphic or secondary-level content simply because it appears in this staff policy. [9]

Contact Risks

Teach age-appropriate boundaries: people online may not be who they claim; ask a trusted adult before communicating or sharing; and tell an adult about frightening, uncomfortable or secret-keeping requests. Children should know they will receive help even if they have broken a rule.

Conduct Risks

Teach kindness, permission before sharing another person's picture or information, privacy and how to seek help about upsetting messages or pictures. Use age-appropriate language and safeguarding responses to children's questions; explicit imagery is never used as teaching material. [9]

Commerce Risks

Teach pupils to ask a trusted adult before clicking adverts, links, purchases or requests for information. Explain scams and persuasive design in simple terms appropriate to the cohort; children should not make online purchases or disclose account information independently.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Early years screen use

EYFS paragraph 3.94 now requires providers to have regard to DfE screen-use guidance from September 2026. Therefore screen-use is limited and has purposeful use, with adult co-engagement and previewed, age-appropriate, advert-free content without scrolling or autoplay. Screens will not replace interaction, play or movement or be used routinely to manage behaviour. Staff will avoid AI tools and AI-enabled toys for early-years children. [6]

The school will work with families on daily screen exposure: avoid screens for under-twos except exceptional use such as a family video call, and aim for no more than one hour across home and the setting for ages two to five, but preferably less. Essential SEND assistive technology is excluded from these limits.

Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils must not use personal phones or similar connected devices during the school day, including breaks. If a device must be brought into school as an exception, it is switched off and handed to the office for secure storage and returned at collection. Planned used with parents/carers will be arranged for any necessary disability, medical or other exceptional access individually. Parents will contact pupils through the school office in an emergency. [7]

Staff use technology in line with the Internet and Acceptable Use Policy and Staff Code of Conduct. Personal phones, cameras, smartwatches and devices with recording or sharing functions are not used around children or in teaching areas and are securely stored in lockers. A risk assessment and agreement needs to be in place for necessary medical devices.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.
- Using whilst in teaching areas.

The Headteacher / DSL will respond to device misuse through safeguarding assessment and the Behaviour Policy, with proportionate action, SEND adjustments and support. Searches, confiscation and examination of devices must follow statutory powers and DfE guidance; this policy creates no additional power to inspect private content. [7, 12]

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' Workops
- Parentmail Communications
- Online resources

Internet access

Adult users must receive the relevant acceptable-use agreement and understand the controls before access. Staff will teach pupils simple rules with parent/carer information provided for support at home.

All staff and pupils will use the approved filtered school network for school activities. Personal mobile data, hotspots, VPNs, proxies or unauthorised accounts must not be used to bypass controls.

Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The Headteacher, DSL and IT Support, with the responsible governor, review provision at least annually and after significant changes or incidents. This will involve assessing pupils' ages, SEND, EAL, vulnerabilities and how devices and services are used, including at home and with AI. [3]

Any filtering failures or harmful content must be reported immediately to the DSL and IT technician who will record checks, outcomes and fixes. A change or temporary exception requires risk assessment, authorisation, a recorded reason, expiry/review date and testing; staff must not disable controls themselves. New devices and services will be checked before issue and after significant changes. [3]

Report deliberate circumvention to the DSL and IT technician for assessment who will consider safeguarding, context and reasonable adjustments as well as any proportionate disciplinary action. Accidental exposure or prompt reporting must not automatically be treated as misconduct.

The DSL coordinates any required reports to police, children's social care, CEOP or the IWF, using their reporting processes. A platform or IWF report does not replace an urgent safeguarding referral. Do not download, screenshot or forward suspected child sexual abuse imagery as evidence. [8]

Filtering and monitoring covers school-managed devices and relevant services, including off-site use. Monitoring must be lawful, necessary, proportionate and transparent, with restricted access, justified retention and a DPIA where required. [3, 10]

Network security

The IT technician maintains managed firewalls, supported software, malware protection and updates. Critical/high-risk vulnerability fixes, CVSS 7 or above fixes and fixes without a severity rating will be applied within 14 days of release, sooner where necessary and devices isloated with unresolved high-risk vulnerabilities. [4]

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technician.

Any access will use individual accounts, strong unique credentials or approved passkeys and appropriate access permissions. MFA must be enabled for staff cloud/remote-access accounts and IT administrators, or an appropriate supported passkey. Compromised credentials will be replaced immediately; routine password changes are not the default. Pupils will be provided with safe, age-appropriate and accessible login arrangements. [4]

Users will inform ICT technician if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff and Volunteer Confidentiality Policy.

Only approved school accounts and secure channels for school business, including remote work must be used. Do not use personal email accounts for pupil, parent or school information. Users must check recipients and protect sensitive information appropriately. Personal-device work access is exceptional and must meet the written approval and security controls in the Internet and Acceptable Use Policy.

Users must report suspicious emails to the Headteacher before deleting evidence needed for an investigation. Do not open suspicious attachments, links or QR codes. Technical detection is not infallible: familiar names, correct spelling or professional presentation do not prove authenticity, especially with AI-generated scams. Staff will teach pupils to ask an adult about unexpected messages, using age-appropriate examples:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

Generative artificial intelligence (AI)

AI use requires an approved purpose and documented assessment of benefits, risks, age restrictions, accessibility, data protection and safeguarding. This will assess embedded AI features as well as stand-alone tools, using the DfE product safety standards. Staff must check outputs for accuracy, bias, suitability and copyright and remain accountable for their use. [5]

Review whether filtering and monitoring can address real-time AI content and record limitations and mitigations. Restrict unapproved tools and features. Supervision and technical safeguards must be in place before any approved pupil use; do not assume a web filter can inspect every chatbot response. [3, 5]

Early-years children must not use AI tools or AI-enabled toys, in line with current screen-use guidance. Older pupils may use AI only in an approved age-appropriate activity with close supervision and compliant provider terms. Unsupervised general-purpose chatbot use and under-age accounts are not permitted. No AI use may impersonate people, fabricate evidence or create sexualised images. [5, 6]

Do not enter personal, sensitive or confidential information, safeguarding records, images or pupil work into an unapproved AI service. Any strictly necessary personal-data use needs documented lawful grounds, suitable contracts, privacy information and a DPIA where required. Do not permit provider model training on school data or pupil work without separate lawful authorisation, including copyright permission where required. [5]

AI must not make safeguarding, disciplinary or other significant decisions about individuals without meaningful authorised human assessment. An approved-service register will be kept and reviewed for changes in features, data use and safety. [5]

Social networking

This is communicated through the Staff Code of Conduct and Internet and Acceptable Use Policy: use authorised school channels, maintain professional boundaries, and do not communicate with pupils through personal social-media accounts. Do not publish abusive, discriminatory or confidential material. These rules do not restrict lawful whistleblowing or safeguarding disclosures.

The school website

The Headteacher oversees website content. Published images and personal information is only for an approved purpose and lawful basis, following recorded permissions and safeguarding restrictions.

Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Acceptable Use Policy.

Remote learning

Only approved remote-learning platforms and school accounts will be used with risk-assessment and arrangements under the Remote Education Policy. Expected conduct and recording arrangements will be explained to families. Filtering and monitoring will be applied to loaned managed devices, alongside an explanation of limitations and information for reporting concerns. Staff will maintain professional boundaries.

Information sharing and privacy

From 30 September 2026, the section 16LA Children Act 2004 information-sharing duty and September 2026 statutory guidance where its criteria are met will be applied. [11]

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technician and the headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The Governing Board, Headteacher and DSL review the policy annually, sooner after significant incidents or changes. Record decisions, actions and outcomes; confirm contacts, alert cover and system arrangements before adoption.

Any changes made to this policy are communicated to all members of the school community

Official Guidance and Source Links

1 Keeping children safe in education 2026
2 Working together to safeguard children 2026
3 DfE filtering and monitoring core standard
4 DfE cyber security core standard
5 DfE generative AI in education
DfE generative AI product safety standards
6 EYFS statutory framework September 2026
DfE early years screen use
7 Mobile phones in schools statutory guidance
8 UKCIS sharing nudes and semi nudes
9 Relationships and health education statutory guidance effective September 2026
Teaching online safety in schools
10 ICO personal data breaches guide
ICO monitoring workers
DfE data protection in schools and the Data Use and Access Act
11 Information sharing statutory guidance
12 Searching screening and confiscation guidance

Appendix 1

Online Safety Long Term Planning Overview

	Term 1	Term 2	Term 3	Term 4	Term 5	Term 6
Nursery						Managing Online Information
Reception	Self-Image and Identity	Online Reputation	Online Bullying	Managing Online Information	Health, Wellbeing and Lifestyle	Privacy and Security
	Online Relationships					Copyright and Ownership
Year 1	Self-Image and Identity	Online Reputation	Online Bullying	Managing Online Information	Health, Wellbeing and Lifestyle	Privacy and Security
	Online Relationships					Copyright and Ownership
Year 2	Self-Image and Identity	Online Reputation	Online Bullying	Managing Online Information	Health, Wellbeing and Lifestyle	Privacy and Security
	Online Relationships					Copyright and Ownership

Online Safety Long Term Planning Objectives

	Nursery	Reception	Year 1	Year 2
Self-Image and Identity		I can recognise, online or offline, that anyone can say 'no'/ 'please stop'/ 'I'll tell'/'I'll ask' to somebody who makes them feel sad, uncomfortable,	I can recognise that there may be people online who could make someone feel sad, embarrassed or upset. If something happens	I can explain how other people may look and act differently online and offline. I can give examples of issues that might make someone feel sad, worried, uncomfortable or frightened; I can give examples of

		embarrassed or upset.	that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust and how they can help.	how they might get help.
Online Relationships		I can recognise some ways in which the internet can be used to communicate. I can give examples of how I (might) use technology with people I know.	I can give examples of when I should ask permission to do something online and explain why this is important. I can use the internet with adult support to communicate with people I know (e.g. video call apps or services) I can explain why it is important to be considerate and kind to people online and respect their choices. I can explain why things one person finds funny or sad online may not always be seen in the same way as others	I can give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky. (e.g. email, online gaming, a pen-pal in another school / country) I can explain who I should ask before sharing things about myself and others online. I can describe different ways to ask for, give or deny my permission online and can identify who to help me if I am not sure. I can explain why I have a right to say 'no' or 'I will have to ask someone'. I can explain who can help me if I feel under pressure to agree to something I am unsure about or don't want to do. I can identify who can help me if something happens online without my consent. I can explain how it may make others feel if I do not ask their permission or ignore their answers before sharing something about them

				online. I can explain why I should always ask a trusted adult before clicking 'yes', 'agree', or 'accept' online
Online Reputation		I can identify ways that I can put information on the internet.	I can recognise that information can stay online and could be copied I can describe what information I should not put online without asking a trusted adult first.	I can explain how information put online about someone can last for a long time I can describe how anyone's online information could be seen by others I know who to talk to if something has been put online without consent or if it is incorrect.
Online Bullying		I can describe ways that some people can be unkind online I can offer examples of how this can make others feel.	I can describe how to behave online in ways that do not upset others and can give examples.	I can explain what bullying is, how people may bully others and how bullying can make someone feel. I can explain why anyone who experiences bullying is not to blame. I can talk about how anyone experiences bullying can get help.
Managing Online Information	I can talk about how to use the internet as a way of finding information online. I can identify devices I could use to access information on the internet	I can talk about how to use the internet as a way of finding information online. I can identify devices I could use to access information on the internet	I can give simple examples of how to find information using digital technologies e.g. search engines, voice activated searching I know/understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe/ a joke I know how to get help	I can use simple keywords in search engines I can demonstrate how to navigate a simple webpage to get information I need (e.g. home, forward, back buttons; links, tabs and sections. I can explain what voice activated searching is and how it might be used, and know it is not real person (e.g. Alexa, Google Now, Siri) I can explain the difference between things that are

			from a trusted adult if we see content that makes us feel sad, uncomfortable, worried or frightened.	imaginary, 'made up', or 'make believe' and things that are 'true' or 'real' I can explain why come information I find online may not be real or true.
Health, Wellbeing and Lifestyle		I can identify rules that help keep us safe and healthy in and beyond the home when I am using technology. I can give some simple examples of these rules	I can explain rules to keep myself safe when using technology both in and beyond the home	I can explain simple guidance for using technology in different environments and settings e.g. accessing online technologies in public places and the home environment. I can say how those rules/guides can help anyone accessing online technologies
Privacy and Security		I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location) I can describe who would be trustworthy to share this information with; I can explain why they are trusted.	I can explain that passwords are used to protect information, accounts and devices I can recognise more detailed examples of information that is personal to someone (e.g. where someone lives and goes to school, family names) I can explain why it is important to always ask a trusted adult before sharing any personal information online, belonging to myself or others.	I can explain how passwords can be used to protect information, accounts and devices. I can explain and give examples of what is meant by 'private' and 'keeping things private' I can describe and explain some rules for keeping personal information private (e.g. creating and protecting passwords) I can explain how some people may have devices in the their homes connected to the internet and give some examples (e.g. lights, fridges, toys, televisions.)
Copyright and Ownership		I know that work I	I can explain why work I	I can recognise that content on

		create belongs to me I can name my work so that others know it belongs to me	create using technology belongs to me I can say why it belongs to me (e.g. I designed it or I filmed it) I can save my work under a suitable title/name so that others know it belongs to me (e.g. filename, name on content) I understand that work made by others does not belong to me even if I save a copy.	the internet may belong to other people. I can describe why other people's work belongs to them.