



Sitwell Nursery & Infant School

Online Safety Policy

Statement of intent

Sitwell Nursery & Infant School understands that using online services is an important aspect of raising educational standards, promoting child 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 children and staff.

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

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, 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.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect children 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 children and staff.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE 'Filtering and monitoring standards for schools and colleges'
- DfE 'Harmful online challenges and online hoaxes'
- DfE 'Keeping children safe in education 2025'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE 'Teaching online safety in school'
- DfE 'Searching, screening and confiscation'
- DfE 'Generative artificial intelligence in education'
- National Cyber Security Centre 'Cyber Security: Small Business Guide'

- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following school policies:

- AI Policy
- Social Media Policy
- Allegations of Abuse Against Staff Policy
- IT Security & AU Policy
- Safeguarding inc Child Protection Policy
- Anti-Bullying Policy
- PSHE Policy
- Relationships & Health Education Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Remote Education Policy

Roles and responsibilities

The governing board is 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.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- 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.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The Headteacher is 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 any deputies 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.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all children can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping children safe.
- Working with the DSL and governing board to update this policy on an annual basis.

The Designated Safeguarding Lead (DSL) is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that children with additional needs face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCo and ICT technicians.
- 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.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- 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.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by children and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- 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 governing board to update this policy on an annual basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.

- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are 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 concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Children are responsible for:

- Adhering to this policy, the ICT Acceptable Use Agreement and other relevant policies.
- 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 the Deputy DSL and the Computing subject leader, where appropriate, and will ensure that there are strong processes in place to handle any concerns about children's 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 email 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 regularly on the topic of remaining safe online.

Handling online safety concerns

Any disclosures made by children 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 Safeguarding inc Child Protection Policy. These are logged on

CPOMS in order to provide an evidence trail and for the DSL to consider a pattern of events.

Staff will be aware that children may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

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 children displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately, the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully; the reasons for sharing the information should be explained to the victim and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Safeguarding inc Child Protection Policy and Disciplinary Policy and Procedures. If the concern is about the Headteacher, it is reported to the chair of governors.

Concerns regarding a child's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police. The school avoids unnecessarily criminalising children, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a child has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

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 children can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND. Cyberbullying against children 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

Children may also use the internet and technology as a vehicle for sexual abuse and harassment. All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this 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, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- 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 children becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the

imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

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 children taking “sides”, often leading to repeat harassment.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child on Child Abuse and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

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 children 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.
- 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)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a child may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

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 children 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 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 children at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any children displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a child relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Safeguarding Policy.

Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in children, e.g. low self-esteem and suicidal ideation. 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.

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 child 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 children, 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 children
- 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 children
- 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 Safeguarding Policy

Where the DSL's assessment finds an online challenge to be putting children at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant children, e.g. those within a particular age range that is directly affected or even to individual children 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 children's 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 children 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 child'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 children are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

In addition, the school will implement a cyber-awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cybercrime. The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Policy.

Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that children are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life. 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.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-Bullying Policy and the Safeguarding Policy.

Online Safety & the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships & Health education
- PSHE
- Computing

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance. Children 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.

Online safety teaching is always appropriate to children's ages and developmental stages. The underpinning knowledge and behaviours children learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem

- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks children may face online are always considered when developing the curriculum. The DSL is involved with the development of the school's online safety curriculum. The school recognises that, while any child can be vulnerable online, there are some children who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. children with additional needs or those who are looked after (LAC).

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 children.

The Computing lead will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of children. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for children?
- Are they appropriate for children's developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL 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 consider the topic that is being covered and the potential that children in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any child who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a child 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 ensures a safe environment is maintained in which children feel comfortable to say what they feel and asking questions, and are not worried about getting into trouble or being judged. If a staff member is concerned about anything children raise during online safety lessons and activities, they will follow the reporting procedure outlined in the Safeguarding Policy.

If a child 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 Safeguarding Policy.

Use of technology in the classroom

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

- Computers
- Laptops
- Tablets/iPads
- Beebots
- Internet
- Cameras
- Google Classroom
- Clevertouch boards

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that children use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Children are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Educating parents

The school works in partnership with parents to ensure children stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of children, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

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 is raised in the following ways:

- Parents' evenings.
- Twilight training sessions.
- Newsletters.
- Online resources, including videos and information in sections of the school website.
- Wake Up Wednesday information sheets

Internet access

Children, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the school office. All members of the school community are encouraged to use the school's

internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

The governing board ensures 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 Headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to children's ages, the number of children using the network, how often children access the network, and the proportionality of costs compared to the risks. 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 governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding. ICT technicians undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate. Requests regarding making changes to the filtering system are directed to the Headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by ICT technicians.

Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes. Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police. The school's network and school-owned devices are appropriately monitored.

All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the appropriate policy.

Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and children are advised not to download unapproved software or open unfamiliar email attachments. Staff members and children report all malware and virus attacks to the ICT technician. All members of staff have their own unique usernames and private passwords to access the school's systems. Staff members are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a

mixture of letters, numbers and symbols to ensure they are as secure as possible. Based on recommendations from the National Cyber Security Centre, staff must set passwords that are three random words e.g. Goingsmellwound1!

Passwords expire after 90 days, after which users are required to change them. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. Users are required to lock access to devices and systems when they are not in use. Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher is informed and decides the necessary action to take.

Emails

Access to and the use of emails is managed in line with the Data Protection Policy, ICT Acceptable Use Agreement and Confidentiality Policy. Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the ICT Acceptable Use Agreement.

Any email that contains sensitive or personal information is only sent using secure and encrypted email. Staff members are required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Generative artificial intelligence (AI)

The school will take steps to prepare children for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit children's ability to access or create harmful or inappropriate content through generative AI. The school will ensure that children are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable. The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Social networking

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy.

The school website

The Headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. The website complies with guidelines for publications including accessibility, data protection, and respect for intellectual property rights, privacy

policies and copyright law. Personal information relating to staff and children is not published on the website. Images and videos are only posted on the website if the provisions in the ICT Acceptable Use Policy are met.

Use of school-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop/Chromebook
- Camera
- Smartphone

Children are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. laptops to use during lessons. School-owned devices are used in accordance with the ICT Acceptable Use Policy. All school-owned devices are password protected. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased. ICT technicians review all school-owned devices on a monthly basis to carry out software updates and ensure there is no inappropriate material or malware on the devices.

Cases of staff members or children found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour, Discipline & Self-Esteem Policy respectively.

Use of personal devices

Personal devices are used in accordance with the Staff Bring Your Own Device Policy. Any personal electronic device that is brought into school is the responsibility of the user. Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of children.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Safeguarding Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the Headteacher will inform the police and action will be taken in line with the Safeguarding Policy.

Due to the young age of our children, personal devices are not used by the children. The Headteacher may authorise the use of mobile devices by a child for safety or precautionary use. Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

Remote learning

All remote learning is delivered in line with the school's Remote Learning Policy. This policy sets out how online safety will be considered when delivering remote education.

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the governing board, Headteacher and DSL review this policy in full on an annual basis and

following any online safety incidents. Any changes made to this policy are communicated to all members of the school community.

*This policy will be reviewed annually during the Spring term.
Spring 2026*