The Lilycroft and St Edmund's Nursery Schools' Federation

Online Safety Policy

Lilycroft Nursery School

for children from two to five

Version: November 2025

Ratified by the Governing Body:

Signed by the Governing Body:

To be reviewed (annually): November 2026 (or before that as necessary)

This policy is about our role in promoting online safety and how we support staff, apprentices, students, volunteers, governors, parents/carers and children themselves in keeping safe online. Please also refer to the Safeguarding and Child Protection Policy and the Data Protection Policy.

The Governors appreciate that electronic communications are an essential element in 21st century life for education, business and social interaction. The Governors also support children in using ICT as part of their learning experience across all curricular areas and believe that if used correctly ICT will teach children the necessary skills that we now all need in a digital world.

Contents:

Statement of intent

The Lilycroft and St Edmund’s Nursery Schools’ Federation understands that using online services is an important aspect of raising educational standards, promoting achievement, and enhancing teaching and learning. The use of online services is embedded throughout both schools; therefore, there are a number of controls in place to ensure the safety of all individuals.

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, 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 children.
- **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 all individuals across our community revolve around these areas of risk. Our federation has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital devices by all children, staff, apprentices, visitors, students and volunteers

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) ‘Filtering and monitoring standards for schools and colleges’
- DfE (2021) ‘Harmful online challenges and online hoaxes’
- DfE (2023) ‘Keeping children safe in education 2023’
- DfE (2023) ‘Teaching online safety in school’
- DfE (2022) ‘Searching, screening and confiscation’
- DfE (2023) ‘Generative artificial intelligence in education’
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
- UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’
- National Cyber Security Centre (2020) ‘Small Business Guide: Cyber Security’
- This policy operates in conjunction with the following federation policies: Technology Acceptable Use Agreement
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Regulation and Behaviour Guidelines
- Disciplinary Policy and Procedure
- Data Protection Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Remote Education Policy

2. Roles and responsibilities

The governing body will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL’s 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 and at regular intervals.
- 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.

- 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 federation policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Executive Head teacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the federation'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 children safe.
- Working with the DSL and governing body to update this policy on an annual basis.
- Working closely with Data Cable to ensure adequate IT support and guidance.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that children with SEND face online.
- Liaising with relevant members of staff on online safety matters.
- Ensuring online safety is recognised as part of the federation's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the federation's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by children and staff, and ensuring all members of the federation community understand this procedure.
- Understanding the filtering and monitoring processes in place in the federation.
- 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.
- Working with the executive head teacher to review this policy.
- Working with the executive head teacher and governing body to update this policy on an annual basis.

Datacable technicians will be responsible for:

- Providing technical support in the development and implementation of the federation’s online safety policies and procedures.
- Implementing appropriate security measures as directed by the executive head teacher.
- Ensuring that the federation’s filtering and monitoring systems are updated as appropriate.

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 individuals may be unsafe online.
- Reporting concerns in line with the federation’s reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Supporting children and families to keep safe online.

3. 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 federation’s approach to online safety and will ensure that there are strong processes in place to handle any concerns about children’ safety online. The DSL should liaise with the police or children’s social care services for support responding to harmful online behaviour.

The importance of online safety is integrated across all the federation’s operations in the following ways:

- Staff and governors receive regular training
- During weekly planning and children’s meetings ICT is discussed as an aid for learning but to emphasise and support online safety.
- Online safety is integrated into learning throughout the curriculum in a developmentally appropriate way.
- Parental involvement workers work with families to further educate on the needs for online safety.
- During internet-safety week the federation will provide a community focus on online-safety.

Handling online safety concerns

Any disclosures made 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 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 specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the executive head teacher, who decides on the best course of action in line with the relevant policies. If the concern is about the executive head teacher, it is reported to the chair of governors.

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

Where there is a concern that illegal activity has taken place, the executive head teacher contacts the police.

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

4. Cyberbullying

Unfortunately, this is a threat to our children, families and our staff, apprentices, students and volunteers and must be considered.

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/ smart watch 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 federation will be aware that certain people can be more at risk of abuse and/or bullying online, such as LGBTQ+ and people with SEND.

Cyberbullying against children, families or staff, apprentices, students and volunteers 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.

5. Child-on-child 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 colleagues and families are less likely to report concerning online sexual behaviours.

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 individuals becoming less likely to report such conduct.

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

The federation will respond 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 will be reported to the DSL, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

6. 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 people who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the child 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.

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 person 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, families, staff, apprentices, students or volunteers 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 and Child Protection 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.

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand the indicators that a person is suffering from challenges in their mental health. Concerns about the mental health of a person will be dealt with in line with the Staff Wellbeing Policy

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

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

8. 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.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst members of the federation, 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 individuals, 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.

9. 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 federation will factor into its approach to online safety the risk that individuals with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about an individual’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 people are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL will ensure that everyone across our federation is taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The DSL will ensure 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.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum through developmentally appropriate teaching and learning.

Our federation will support families, apprentices/students/volunteers, children and staff to keep safe online.

Our children are taught what to do if something they see or hear makes them feel uncomfortable.

As developmentally appropriate, 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, device or app they are using.

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

Relevant members of staff, e.g. the SENDCO, will work to ensure the curriculum is tailored so that children who may be more vulnerable to online harms, e.g. children with SEND and CLA, receive the information and support they need and their parents/carers have access to additional support.

The federation 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.

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

Before conducting an activity on online safety, the practitioners and DSL will consider the topic that is being covered and the potential that an individual may 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 individual who may be especially impacted by a lesson or activity. A safe environment is maintained in which everyone feels 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 an individual raises they will make a report in line with the Safeguarding and Child Protection Policy.

12. Use of technology in the classroom

Lots of teaching and learning regarding technology with young children is via cause and effect toys and equipment, however a wide range of smart technology will be used across the federation, including but not limited to the following:

- Computers
- Interactive Screens

- Laptops
- IPads
- IPods
- Internet
- Email
- Cameras
- School Mobile Phones

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that children and families use these platforms at home, practitioners will review and evaluate the resource and ensure that any internet-derived materials are used in line with copyright law.

Children will be supervised when using online materials– this supervision is suitable to their age and ability.

13. Use of smart technology

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

Technology is progressing rapidly and the federation will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and their related threats.

Staff, families and visitors entering our schools are likely to have their own devices and these need to be considered carefully to prevent risks and keep children safe. These may include personal mobile phones and smart watches. Whilst we do not allow personal mobile phones around children, smart watches are harder to limit and the updates they bring can provide further risks.

Inappropriate use of smart technology may include:

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

Children will not be permitted to use personal smart devices or any other personal technology whilst in the Nursery.

The federation will address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The federation will consider the 4Cs (content, contact, conduct and commerce) when educating everyone about the risks involved with the inappropriate use of smart technology.

14. Educating families

Due to the very young age of our children, working with families is crucial to keep children safe online.

Families will be made aware of the various ways in which they and 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, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

We try to raise awareness of issues that may relate to children's use of electronic information and offer the following guidance:

The Internet offers a means to learn, share and communicate in a variety of different ways. The federation supports children to use computers and tablets as part of their learning experience; we talk to children about Internet safety, and make sure that the sites children access when they are in the school are safe. Parents and carers need to take equal care at home:

- Ask your child to use the computer/ laptop/ tablet/ mobile phone/ smart watch/ interactive sound system (e.g. Alexa) in a communal area such as a family room where you can keep an eye on what your child is accessing on the internet.
- Use an appropriate filtering system/parental control to minimise opportunities to access unsuitable material – if you are in doubt about the filtering system you have in place you can contact your service provider to discuss how you can limit access to inappropriate internet sites e.g. pornography or gambling websites.
- Bookmark or create a list of favourite sites and apps, so you and your child can easily find them and not get distracted by pop ups or adverts.
- Beware of in app purchases (optional extras within games that you have to pay for) – use parental controls to disable in-app purchasing.

Get your child into good habits early – make it a rule that:

- Your child always checks with an adult before they use the internet.
- Your child only talks online to people they know.
- Your child never tells anyone how old they are, where they live, or arranges to meet someone they don't know.
- Your child only uses the internet to look for things they know they are allowed to look at. If they're not sure they should check with an adult before they search.
- Your child is polite when they talk or post things on the Internet and doesn't say things that will upset people.
- Limit the time that your child is online, so they have chance to do other things too.

Some useful questions to ask your child are:

- What do you like about this … (tablet/phone etc.)?
- Can you teach me how to do that?
- What should you do if you don't like something you see/hear?
- How do you feel now it's time to stop using this … (tablet/ phone etc)?

Your child needs to know that if they see or hear anything that worries or upsets them they must ask a familiar adult for help straight away. More information is available at https://www.getsafeonline.org/

Other useful links: Childnet, CEOP Thinkuknow, UK Safer Internet Centre.

Families 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.

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

- Parents' meetings
- Training sessions
- Newsletters / handouts
- Online resources
- Verbal guidance through their key person

15. Internet access

Children, staff and other members of the federation community will only be granted access to the school's internet network once they have received an induction.

All members of the federation community will be 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 onsite.

16. Filtering and monitoring online activity

The governing body will ensure the federation'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 body will ensure 'over blocking' does not lead to unreasonable restrictions as to what children 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 federation's safeguarding needs.

All practitioners are aware that they cannot depend entirely on the filtering and monitoring set up and need to be proactive in looking out for sites that might cause our children harm. They need to report any of these immediately to the DSL.

The executive head teacher and Data Cable ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the federation implements will be 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. Data Cable ICT technicians will undertake checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the executive head teacher. Prior to making any changes to the filtering system, Data Cable ICT technicians and the DSL will conduct a risk assessment. Reports of inappropriate websites or materials will be made to Data Cable ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and Data Cable ICT technicians, who will escalate the matter appropriately.

The federation's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date, reviewed and managed by Data Cable ICT technicians as directed by the executive head teacher. Firewalls will be switched on at all times.

Staff, apprentices, students, volunteers and children 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 Data Cable ICT technicians and the executive head teacher.

All members of staff will have their own unique usernames and private passwords to access the federation's systems.

Users will inform Data Cable ICT technicians if they forget their login details, who will support the user to reset these. 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 executive head teacher 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.

18. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy.

Staff will be given an approved school email account. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to Data Cable ICT technicians. The federation's monitoring system can detect inappropriate links, malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources should be deleted without being opened.

19. Generative artificial intelligence (AI)

The federation will take steps to prepare individuals for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately.

The federation will ensure its IT system includes appropriate filtering and monitoring systems to limit a person's ability to access or create harmful or inappropriate content through generative AI.

The federation will ensure that children are not accessing or creating harmful or inappropriate content, including through generative AI.

The federation will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The federation 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.

20. Social networking

Social networking is an important part of the 21st century and can be an effective tool to communicate with families, however this needs to be achieved with safety in mind.

Social media accounts for the school will be created and maintained by the Admin Team or Parental Involvement Workers, who will ask for contributions from other staff members. A school-based social media account will be entirely separate from any personal social media accounts held by staff members and will be linked to an official school email account.

When setting up a school social media account, consideration will be given to the following:

- The purpose of the account
- Whether the overall investment will achieve the aim of the account
- The level of interactive engagement with the site
- Whether pupils, staff, parents or members of the public will be able to contribute content to the account
- How much time and effort staff members are willing to commit to the account
- How the success of the account will be evaluated

All posts made to school social media accounts will not breach copyright, data protection or freedom of information legislation.

The school's social media accounts will comply with the platform's rules.

Staff will ensure that their posts meet the following criteria:

- The post does not risk bringing the school into disrepute
- The post only expresses neutral opinions and does not include any personal views
- The post uses appropriate and school-friendly language
- The post is sensitive towards those who will read it, and uses particularly neutral and sensitive language when discussing something that may be controversial to some
- The post does not contain any wording or content that could be construed as offensive
- The post does not take a side in any political debate or express political opinions
- The post does not contain any illegal or unlawful content

To post photos and videos of individual children the federation will obtain consent from families during admission. Consent provided for the use of images and videos only applies to school accounts – staff, pupils and parents are not permitted to post any imagery or videos on personal accounts. The admin team, parental involvement workers and each class will be aware of children who do not have this permission.

Only school-owned devices will be used to take images and videos of the federation community. Only appropriate images and videos of pupils will be posted in which they are suitably dressed.

Parents are able to comment on or respond to information shared via social media sites; however, parents should do so in a way which does not damage the reputation of the school.

Parents will be asked not to share any photos or personal details of pupils when commenting on school social media sites, nor post comments concerning other pupils or staff members.

Staff will not be prohibited from having personal social media accounts; however, it is important that staff protect their professional reputation by ensuring they use personal social media accounts in an appropriate manner.

Staff will be required to adhere to the following guidelines when using personal social media accounts:

- Staff members will not access personal social media platforms during working hours.
- Staff members will not use any school-owned mobile devices to access personal accounts.
- Staff will not 'friend', 'follow' or otherwise contact families within the federation (only known to them through school) through their personal social media accounts. If a parent attempts to 'friend' or 'follow' a staff member, they will report this to a member of the Senior Leadership Team.
- Staff members will ensure the necessary privacy controls are applied to personal accounts and will avoid identifying themselves as an employee of the school on their personal social media accounts.
- Staff will ensure it is clear that views posted on personal accounts are personal and are not those of the school.
- Staff will not post any content online that is damaging to the school, its staff or pupils.
- Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.
- Staff members will not post anonymously or under an alias to evade the guidance given in this policy.
- Staff will not post comments about the school, pupils, parents, staff or other members of the school community.
- Staff members must never post photos or videos of children from the Federation (only known to them through school) on their personal accounts.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal. Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
- Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.

21. The school website

The executive headteacher will be responsible for the overall content of the website for both schools – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

22. Use of devices

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

Each practitioner will be responsible for this device and for keeping the device safe. Any misuse will be acted upon at the discretion of the executive headteacher.

The use of school cameras is being phased out and no more will be ordered. School sim-free mobile phones will be the chosen device for practitioners to use in the rooms to aid teaching and learning. These must be pin protected and Data Cable ICT technicians will ensure Multi Factor Authentication and a Yubikey is set up on each device for an added level of security. Any cameras still in use, Ipods and sim-free mobile phones must be kept on the designated person (through use of a school bum-bag ideally). During breaks and out of working hours these must be locked away. Once photos and videos have been used for their intended purse, for example for an observation, they must be deleted from the device. The staff member is responsible for deleting these images.

School devices may be taken off the premises to capture learning during trips and visits.

If a device is lost (on or off site) this must be reported immediately to the executive headteacher who will, with the support of Data Cable Technicians, trace the device and remotely remove any photos, videos and personal information from the device.

Ipods and Ipads will follow the same safety measures as sim free phones.

The use of personal devices on the school premises and for the purposes of school work will be at the discretion of the Executive Head teacher.

Some designated members of staff will be provided with a school mobile phone. Individual risk assessments are carried out for each of these.

As soon as a device is found to be missing/stolen, staff must report this to SLT & Datacable immediately upon the loss/theft to request that the managed device be remotely wiped of school-sensitive data. Failure to report the loss/theft will breach data protection guidelines.

Two-factor authentication (2FA) is required on all school mail accounts to ensure they are secure and protected.

23. Remote learning

Any remote learning will be offered through the school’s website, through the Famly App. And also through the 50 Things to Do Before You’re Five website and App.

24. Monitoring and review

The federation recognises that the online world is constantly changing; therefore, the DSL, Data Cable ICT technicians and the Executive head teacher conduct frequent reviews of this policy to evaluate its effectiveness.

The governing board, head teacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is November 2026.

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