Online Safety
(Whole School including EYFS)

Independent Day School

Our Lady of Sion School

Last Reviewed:	August 2025
Frequency of Review:	Annual
Next Review Due:	August 2026

Introduction and Statement of Intent

Our Lady of Sion School recognises that the safe use of online services is a critical part of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. Online technologies are fully embedded in our curriculum and school operations; therefore, robust measures are in place to ensure the safety of pupils and staff.

The range of online safety issues is wide, but for clarity, they can be categorised into four key areas of risk:

a) Content – exposure to illegal, inappropriate, or harmful material, such as:

- Pornography
- Racism and discrimination
- Misogyny
- Self-harm and suicide
- Radicalisation and extremism
- Misinformation, disinformation (including fake news), and conspiracy theories

b) Contact – harmful interactions with other users, including:

- Peer-to-peer pressure
- Commercial advertising
- Adults posing as children or young adults to groom or exploit pupils for sexual, criminal, financial, or other purposes

c) Conduct – personal online behaviour that increases the likelihood of harm, such as:

- Making, sending, and receiving explicit messages
- Consensual and non-consensual sharing of nudes or semi-nudes
- Sharing pornography or other explicit content
- Online bullying

d) Commerce – exposure to online risks, including:

- Online gambling
- Inappropriate advertising
- Phishing
- Financial scams

The measures implemented at Our Lady of Sion School aim to address all four areas of risk and provide a safe digital environment for our school community.

This policy establishes the framework to ensure the appropriate and safe use of the internet and digital devices by pupils and staff, protecting all members of the school community while supporting effective teaching, learning, and school operations.

1. Legal Framework

1.1 Relevant Legislation and Statutory Guidance

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

- **Online Safety Act 2023**
- **Voyeurism (Offences) Act 2019**
- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **DfE (2025): Filtering and monitoring standards for schools and colleges**
- **DfE (2021): Harmful online challenges and online hoaxes**
- **DfE (2025): Keeping Children Safe in Education (KCSIE)**
- **DfE (2023): Teaching online safety in school**
- **DfE (2022): Searching, screening and confiscation**
- **DfE (2025): Generative artificial intelligence in education**
- **DCMS & UKCIS (2024): Sharing nudes and semi-nudes – advice for education settings**
- **UKCIS (2020): Education for a Connected World – 2020 edition**
- **NCSC (2020): Small Business Guide: Cyber Security**

1.2 Associated School Policies/Procedures

This policy operates alongside and should be read in conjunction with:

- Social Media Policy
- Low Level Concerns Policy
- Acceptable Use Agreement Forms
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Photography and Images Policy
- Prevent Duty Policy
- Safe Use of AI Policy

2. Roles and Responsibilities

2.1 Governing Board

The governing board is responsible for:

- Ensuring the policy is effective and legally compliant.
- Ensuring the DSL's remit covers online safety.
- Conducting an annual policy review.
- Keeping up to date with online safety issues.
- Ensuring all staff receive induction and ongoing safeguarding training, including online safety.
- Overseeing filtering and monitoring systems and reviewing their effectiveness annually.
- Embedding online safety approaches in relevant school policies.
- Ensuring compliance with DfE digital and technology standards, particularly safeguarding, filtering, and monitoring.

2.2 Headteacher

The headteacher is responsible for:

- Integrating online safety throughout school policies, curriculum, training, and safeguarding.
- Supporting the DSL with time and resources.
- Providing staff with regular online safety training.
- Auditing and evaluating online safety practices.
- Engaging with parents regarding online safety measures.
- Conducting half-termly light-touch reviews of this policy with the DSL and ICT providers.
- Updating this policy annually with the DSL and governing board.
- Assigning responsibilities for filtering and monitoring systems.
- Appointing an SLT Digital Lead as per the Cyber-security Policy.

2.3 Designated Safeguarding Lead (DSL) – currently the Digital Lead (2025-2026)

The DSL is responsible for:

- Leading online safety across the school.
- Undertaking training, including risks for pupils with SEND.
- Liaising with staff, SENCO, and ICT providers on online safety.
- Integrating online safety into safeguarding practices and remote learning.
- Establishing clear procedures for reporting online safety incidents.
- Understanding and overseeing filtering and monitoring processes.
- Providing specialist knowledge on content management and restricted access.
- Maintaining records of incidents and trends, reporting to the governing board termly.

2.4 ICT External Support Providers

ICT providers are responsible for:

- Providing technical support for online safety policies.
- Implementing security measures as directed by the headteacher.
- Updating filtering and monitoring systems.
- Supporting half-termly reviews of this policy.
- Offering specialist guidance on filtering and monitoring software.

2.5 All Staff

All staff are responsible for:

- Maintaining ICT system and data security.
- Modelling good online behaviour and professionalism.
- Recognising and reporting online safety concerns.
- Embedding online safety into the curriculum, as relevant.

2.6 Pupils

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and related policies.
- Seeking help from staff regarding online safety concerns.
- Reporting online safety incidents in line with this policy.

3. Managing Online Safety

3.1 Whole-School Approach

Our Lady of Sion School recognises that technology is a significant factor in many safeguarding and wellbeing issues affecting young people, particularly due to social media and the increasing prevalence of internet use among pupils.

The Designated Safeguarding Lead (DSL) holds overall responsibility for online safety, supported by deputies and the headteacher, and will ensure strong processes are in place to respond to concerns regarding pupils' online safety. The DSL will liaise with the police or children's social care services where necessary, particularly in cases of harmful online sexual behaviour.

Online safety is embedded across all aspects of school life, including:

- Staff and governors receiving regular training on online safety.
- Staff receiving timely updates on online safety developments, guidance, and legislation via email.
- Curriculum integration, ensuring pupils learn about online safety across subjects.
- Termly assemblies focused on safe online behaviour.
- Ongoing communication with parents regarding relevant online safety matters.

3.2 Handling Online Safety Concerns

Disclosures by Pupils

- Any disclosures by pupils concerning online abuse, harassment, or exploitation—whether as victims or bystanders—will be managed in line with Safeguarding Policy.

Recognising Harmful Behaviour

- Staff will acknowledge that harmful online sexual behaviour often develops along a continuum, and that early intervention can prevent escalation.
- Pupils displaying harmful behaviours may themselves be victims of abuse and will be supported appropriately.

Victim Safeguarding and Confidentiality

- Where a victim requests that no one be informed, the DSL will balance the pupil's wishes with their safeguarding duty.
- Confidentiality will not be guaranteed; information may be shared lawfully (e.g., under UK GDPR if necessary, in the public interest).
- If reporting abuse to social care or the police against a victim's wishes, the process will be handled sensitively, explaining the reasons and offering specialised support.
- Parents of victims will be actively engaged in discussions about safeguarding measures and the handling of reports.

Concerns About Staff Behaviour

- Concerns relating to a staff member's online conduct will be reported to the headteacher, who will follow relevant school policies.
- Concerns regarding the headteacher will be reported to the chair of governors.

Concerns About Pupils' Behaviour

- Concerns relating to pupils' online conduct will be reported to the DSL, who will investigate alongside relevant staff (e.g., headteacher, ICT support providers) and manage cases under the appropriate policies, such as the Behaviour Policy or Safeguarding Policy.

Illegal Activity

- Where illegal activity is suspected, the headteacher will contact the police.
- The school will aim to avoid unnecessarily criminalising pupils, for example, in cases of developmental curiosity such as sharing indecent images of themselves.
- The DSL will decide where discretion is appropriate, in line with safeguarding policy.

Recording Incidents

- All online safety incidents and the school's responses will be logged and maintained by the DSL via the CPOMS recording platform.

4. Cyberbullying

4.1 Definition

Cyberbullying is a form of bullying that takes place through digital technology. It may include, but is not limited to:

- 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 appear responsible.
- Threatening or bullying emails, possibly sent using a pseudonym or another person's name.
- Unpleasant or harmful messages sent via instant messaging platforms.
- Unpleasant or defamatory content posted on blogs, personal websites, or social networking sites.
- Abuse between young people in intimate online relationships (teenage relationship abuse).
- Discriminatory bullying online, including homophobia, racism, misogyny, and misandry.

4.2 Vulnerable Groups

Our Lady of Sion School recognises that some pupils are at greater risk of online abuse or bullying, including, but not limited to:

- Pupils who identify as LGBTQ+.
- Pupils with special educational needs and disabilities (SEND).

4.3 School Response

Cyberbullying directed at pupils or staff will not be tolerated under any circumstances. All incidents will be handled promptly, proportionately, and effectively, in line with the school's Anti-Bullying Policy.

5. Child-on-child Sexual Abuse and Harassment

5.1 Overview

Pupils may use the internet and digital technologies as a vehicle for sexual abuse and harassment. Staff understand that such abuse can occur both inside and outside of school, and both online and offline. Staff will remain vigilant to the fact that pupils are often reluctant to report concerning sexual behaviours online, particularly on platforms that are inappropriate for their age.

5.2 Examples of Online Harmful Sexual Behaviour

Staff will be alert to the following behaviours, which constitute online harmful sexual behaviour:

- Threatening, facilitating, or encouraging sexual violence.
- **Upskirting** – taking a picture underneath a person's clothing without consent, with the intention of viewing their genitals, breasts, or buttocks.
- Sexualised online bullying, including sexual jokes or taunts.
- Unwanted and unsolicited sexual comments or messages.
- Consensual or non-consensual sharing of sexualised imagery.
- Abuse within intimate online relationships (teenage relationship abuse).

5.3 Zero-Tolerance Approach

All staff will uphold and promote a zero-tolerance approach to sexually harassing or abusive behaviour. Attempts to minimise such conduct, or dismiss it as "banter" or harmless, will not be accepted. Staff understand that tolerating or trivialising these behaviours can foster a school culture in which abuse is normalised, reducing the likelihood of pupils reporting concerns.

5.4 Legal Considerations

Staff will remain aware that creating, possessing, or distributing indecent imagery of children (i.e., individuals under 18) is a criminal offence, even where:

- The imagery is created, possessed, or distributed with the consent of the child depicted.
- The imagery is created, possessed, or distributed by the child themselves.

5.5 School Response

The school recognises that interactions between victims and alleged perpetrators are likely to continue with the use of social media after an incident is reported, often involving other pupils taking “sides” and escalating harassment.

The school will respond to these incidents in line with the:

- Child-on-child Abuse as covered in the Safeguarding Policy
- Social Media Policy

All concerns regarding online child-on-child sexual abuse and harassment will be addressed, regardless of whether the incident occurred on school premises or involved school equipment.

Concerns will be reported to the DSL, who will investigate in line with the Child-on-child advice as stated in the Safeguarding Policy.

6. Grooming and Exploitation

6.1 Grooming

Grooming is defined as the process by which 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 subjected to grooming are unlikely to report it due to:

- Developing feelings of loyalty, admiration, or love towards their groomer.
- Experiencing fear, distress, and confusion.
- Being manipulated into secrecy.

Staff must remain alert to potential indicators of grooming, including where a pupil is:

- Being secretive about online activity.
- Claiming to have an older boyfriend or girlfriend who does not attend the school and is unknown to close friends.
- Possessing unexplained money or new items, such as clothes or electronic devices.

The DSL will ensure that staff receive training on recognising the signs of online grooming and how to respond appropriately.

6.2 Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

- CSE often involves physical sexual abuse or violence but may also include online elements, such as coercion or encouragement to behave in sexually inappropriate ways via the internet. Pupils may be groomed online into wider exploitation networks, e.g., production of child sexual abuse material, forced child prostitution, or sexual trafficking.

- CCE occurs when children are manipulated or coerced into committing crimes for the benefit of others, e.g., drug transportation, shoplifting, or violent acts. Increasingly, this process begins online through grooming and manipulation.

Where staff suspect CSE or CCE, concerns must be reported to the DSL immediately, who will manage the case in line with the Safeguarding Policy.

6.3 Radicalisation

Radicalisation is the process by which individuals come to support terrorism or extremist ideologies. This may occur through:

- Direct recruitment – extremists identifying and contacting young people online to involve them in terrorist activities.

- Exposure to extremist propaganda – pupils being influenced by violent ideological content online.

Children targeted for radicalisation are often groomed to believe extremists have their best interests at heart, increasing susceptibility to adopting harmful ideologies.

Staff will be aware of factors that may increase vulnerability to radicalisation, as outlined in the Prevent Duty Policy, and will exercise vigilance when pupils display concerning indicators.

Where radicalisation is suspected, staff must report concerns to the DSL without delay, who will act in accordance with the Prevent Duty Policy.

7. 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 health, either positively or negatively.

The DSL will ensure that training is provided to help staff:

- Understand popular social media platforms and terminology.

- Recognise the ways in which social media and the internet can affect mental health.

- Identify indicators that a pupil may be experiencing mental health challenges.

Concerns regarding a pupil's mental health will be addressed in line with the school's Pupil Mental Health and Wellbeing Policy

8. Online Hoaxes and Harmful Online Challenges

For the purposes of this policy:

- An "online hoax" is a deliberate lie designed to seem truthful, usually intended to scare or distress those who encounter it and spread via social media platforms.

- "Harmful online challenges" are challenges aimed at young people that involve recording oneself participating, sharing the video online, and daring others to do the same. A challenge becomes harmful when it could put participants at risk, either directly (through the activity itself) or indirectly (through online distribution and potential exploitation), taking into account the pupil's age and how they are depicted.

Where staff suspect a harmful online challenge or hoax is circulating among pupils, they must report it to the DSL immediately.

The DSL will:

- Conduct a case-by-case assessment of any reported harmful online content.
- Establish the scale and nature of the risk to pupils, and whether it is local, regional, or national.
- Consult with the Local Authority (LA) if the risk is primarily local to prevent further spread.

Before responding to a hoax or challenge, the DSL and headteacher will ensure that any response:

- Follows advice from reliable sources, e.g., the UK Safer Internet Centre.
- Avoids unnecessarily scaring or distressing pupils.
- Does not inadvertently encourage pupils to seek out the content.
- Is proportional to the actual or perceived risk.
- Provides practical help to pupils at risk.
- Is appropriate to the pupils' age and developmental stage.
- Is supportive and in line with the Safeguarding Policy.

If a harmful online challenge is assessed as putting pupils at risk, the DSL will address it directly with relevant pupils, e.g., specific age groups or individual pupils at risk.

A school-wide approach to highlighting a hoax or challenge will only be taken when the risk of increasing exposure is carefully considered and mitigated.

9. Cyber-crime

Definition

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

1. **Cyber-enabled** – Crimes that can also occur offline but are made easier, faster, or larger-scale online. Examples include:
    - Fraud
    - Purchasing or selling illegal drugs
    - Sexual abuse and exploitation
2. **Cyber-dependent** – Crimes that can only occur online or using a computer. Examples include:
    - Making, supplying, or obtaining malware
    - Illegal hacking
    - 'Booting' (overwhelming a network, computer, or website with internet traffic to render it unavailable)

School Response

- The school recognises that pupils with particular technological skills or interests may be at risk of becoming involved in cyber-crime, whether deliberately or inadvertently.

- Where there are concerns about a pupil's use of technology, the DSL will consider a referral to the Cyber Choices programme, which aims to divert at-risk children towards positive and safe uses of their skills.
- The DSL and headteacher will ensure that pupils are 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 provided to staff includes elements of online safety, including:
  - How the internet can facilitate abuse and exploitation.
  - The expectations, roles, and responsibilities relating to filtering and monitoring systems.
- All staff will be made aware that pupils are at risk of abuse both online and in person, and that such abuse may occur concurrently across online channels and daily life.
- Training will also include a specific focus on harmful online narratives, including:
  - Misinformation
  - Disinformation
  - Conspiracy theories
- Staff will be trained to recognise signs of influence or vulnerability among pupils and to respond appropriately to disclosures or concerns. Training will equip staff with the knowledge and confidence to:
  - Identify signs of online harm
  - Respond effectively to concerns
  - Support pupils in developing critical thinking skills and safe online behaviours
- Staff will be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

11. Online Safety and the Curriculum

Online safety is embedded throughout the curriculum, particularly in the following areas:

- RSHE
- Relationships and Health Education
- PSHE
- Skills for Life (Secondary School)
- ICT
- Assemblies

Teaching on online safety is always appropriate to pupils' ages and developmental stages. Pupils are taught the underpinning knowledge and behaviours that help them navigate the online world safely and confidently, regardless of device, platform, or app.

Core Knowledge and Behaviours

Pupils will learn to:

- Evaluate online content critically
- Recognise techniques used for persuasion
- Understand acceptable and unacceptable online behaviour
- Identify online risks
- Know how and when to seek support
- Develop knowledge and behaviours aligned with the government's online media literacy strategy

The curriculum is developed with consideration of the online risks pupils may face, reflecting the ever-evolving nature of digital spaces. Online safety education addresses four key categories of risk: content, contact, conduct, and commerce.

Content Risks

Pupils are taught to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. Lessons include discussions on:

- Pornography
- Racism, misogyny, anti-Semitism
- Self-harm, suicide
- Radicalisation and extremism
- Misinformation, disinformation, and conspiracy theories

Pupils will learn to question sources, verify information, and understand the dangers of engaging with harmful content.

Contact Risks

Pupils are educated about the dangers of interacting with others online, including:

- Peer pressure and commercial exploitation
- Grooming tactics by adults posing as peers
- Recognising unsafe interactions
- Using privacy settings effectively
- Reporting concerning behaviour to trusted adults or platforms

Conduct Risks

Pupils are guided on how their online behaviour affects themselves and others, including:

- Creating, sharing, or receiving explicit images (consensual and non-consensual)
- Online bullying via social media or messaging platforms
- Understanding the legal and emotional consequences of harmful behaviour

Commerce Risks

Pupils learn about online commercial risks, such as:

- Online gambling
- Exposure to inappropriate advertising
- Financial scams and phishing
- Protecting personal and financial information
- Seeking help for suspicious online activity

Curriculum Development and Support

- The DSL is involved in developing the online safety curriculum.
- Pupils may be consulted to provide insight into their online behaviours and experiences.
- Staff such as the SENCO and designated teacher for LAC will ensure the curriculum is tailored for vulnerable pupils, including those with SEND or LAC status.
- Lessons may be personalised or contextualised in response to harmful online behaviour observed in pupils.

External Resources and Visitors

- Class teachers review external resources prior to use to ensure appropriateness for the cohort.
- External visitors may be invited to support the curriculum; the headteacher and DSL will ensure suitability and appropriateness.

Safeguarding Considerations

- Prior to lessons on online safety, the class teacher and DSL will consider the potential impact on pupils who may have experienced online harm.
- Lessons are planned carefully to avoid publicising the abuse of any pupil.
- A safe environment is maintained where pupils feel comfortable expressing themselves and asking questions without fear of judgement.
- Any concerns raised during lessons are reported in line with the Safeguarding Policy.
- Disclosures made following online safety lessons are handled according to the reporting procedure in the Child Protection and Safeguarding Policy.

12. Use of Technology in the Classroom

- A wide range of technology may be used to support teaching and learning, including:
    - Computers
    - Laptops
    - Intranet
    - Email
- Before using any websites, tools, apps, or other online platforms in the classroom—or recommending that pupils use them at home—class teachers will review and evaluate the resource for suitability. All internet-derived materials must be used in accordance with copyright law.
- Pupils will be supervised when using online materials during lessons. The level of supervision will be appropriate to their age, developmental stage, and ability.

13. Use of Smart Technology

- While the school recognises that smart technology can provide educational benefits, it also carries potential risks that the school will actively manage.
- Pupils will be educated on the acceptable and appropriate use of personal devices and must adhere to the school's Acceptable Use Agreement for Pupils. Staff will use all smart and personal technology in accordance with the school's policies.
- The school acknowledges that pupils' unrestricted access to the internet via mobile networks may lead to misuse of technology in ways that breach the Acceptable Use Agreement. Examples of inappropriate use include:
  - Using mobile or smart technology to sexually harass, bully, troll, or intimidate peers.
  - Sharing indecent images, both consensually and non-consensually.
  - Viewing and sharing pornography or other harmful content.
- Pupils are not permitted to use smart devices or any personal technology while on the school premises.
- Where serious misuse occurs, the school will apply disciplinary measures in line with the Behaviour Policy. Assemblies may be held, when appropriate, to address specific concerns and to emphasise the importance of responsible smart technology use.
- The school will maintain awareness of the latest devices, apps, platforms, trends, and associated risks. In educating pupils and enforcing disciplinary measures, the school will consider the four key categories of online risk—Content, Contact, Conduct, and Commerce (4Cs).

14. Educating Parents

- The school will work in partnership with parents to ensure pupils remain safe online both at school and at home. Parents will be provided with clear information about the school's approach to online safety and their role in supporting their child's digital wellbeing.
- At the start of each academic year, parents will receive a copy of the Acceptable Use Agreement and are encouraged to review it with their child to ensure they understand both the expectations and the consequences of misuse.
- Parents will be made aware of the various online risks their children may face, including, but not limited to:
  - Child sexual abuse, including grooming.
  - Exposure to radicalising or extremist content.
  - Sharing or receiving indecent imagery (e.g., sexting).
  - Cyberbullying.
  - Exposure to age-inappropriate content, such as pornography.
  - Exposure to harmful content, including material that encourages self-harm or destructive behaviour.
- The school will provide guidance on ways parents can help prevent access to harmful content at home, such as using parental controls and monitoring online activity.
- Parental awareness and engagement will be promoted through a variety of channels, including:
  - Parents' evenings.

    - Twilight training sessions.
    - Newsletters and updates.
    - Signposting to reliable online resources.

15. Internet Access

- Access to the school's internet network will only be granted to pupils, staff, and other members of the school community once they have read and signed the Acceptable Use Agreement. A record of all users granted internet access will be maintained and overseen by the Digital Lead/DSL.
- All members of the school community are encouraged to use the school's internet network rather than personal mobile data (3G, 4G, 5G), as the school network includes appropriate filtering and monitoring systems to ensure safe and responsible internet use.
- Mobile phone use is not permitted within the school.

16. Filtering and Monitoring Online Activity

- The governing board will ensure that the school's ICT network has appropriate filtering and monitoring systems in place, in line with the **DfE's Filtering and Monitoring Standards for Schools and Colleges**. Systems will be designed to protect pupils while avoiding over-blocking, ensuring that online teaching and learning are not unreasonably restricted.
- The DSL will ensure that specific roles and responsibilities are assigned for the management of filtering and monitoring systems to meet the school's safeguarding requirements.
- The headteacher and external ICT support providers will undertake a risk assessment to determine the appropriate level of filtering and monitoring, scaled to meet the safeguarding needs of all pupils. External ICT support providers will carry out regular checks to ensure the systems remain effective and appropriate.
- Requests to make changes to the filtering system must be directed to the **headteacher**. Any proposed changes will be assessed for risk by both the DSL and ICT external support providers, and all changes will be formally recorded. Reports of inappropriate websites or materials will be investigated immediately by ICT support.
- Deliberate breaches of the filtering system will be escalated as follows:
    - **Pupils:** Disciplined in line with the Behaviour Policy.
    - **Staff:** Disciplined in line with the Disciplinary Policy and Procedure.
- Accessing illegal material, whether inadvertently or deliberately, will be reported immediately to the relevant authorities, such as the Internet Watch Foundation (IWF), CEOP, and/or the police.
- The school's network and school-owned devices will be monitored appropriately, and all users will be informed about how and why monitoring occurs. Any concerns identified through monitoring will be reported to the DSL and managed according to the **Safeguarding Policy**.
- All staff will receive regular training on the operation and purpose of filtering and monitoring systems, including their safeguarding responsibilities. Personal devices connected to the school network will be subject to the same filtering and monitoring standards.
- Filtering and monitoring systems will undergo a formal review at least annually to assess their effectiveness and relevance.

17. Network Security

1. Technical Security Measures

- Anti-virus software will be kept up-to-date and managed by external ICT support providers.
- Firewalls will always be switched on and reviewed weekly for updates and proper operation.

2. User Responsibilities

- Staff and pupils must not download unapproved software or open unfamiliar attachments.
- Malware or virus incidents must be reported immediately to ICT external support providers.
- All users will have unique usernames and private passwords:
    - Staff and pupils must keep passwords private.
    - Passwords will have minimum/maximum length requirements and include letters, numbers, and symbols.
    - Users must report forgotten login details to ICT support, who will provide alternative access.
    - Sharing login details or impersonating another user is prohibited; breaches will be reported to the headteacher.
- Devices and systems must be locked when not in use.

3. Management and Oversight

- The SLT digital lead, in coordination with the DSL, will oversee network security measures.

18. Email Accounts and Security

1. Email Accounts

- Staff and pupils will only use school-approved email accounts for school-related work.
- Personal email accounts are not permitted on the school site.
- Sensitive or personal information must be sent using secure and encrypted emails.
- Users must have read and agreed to the Acceptable Use Agreement before being authorised to access the school email system.

2. Spam and Security Awareness

- Staff and pupils must block spam or junk mail and report any suspicious emails immediately.
- The school monitoring system will detect inappropriate links, malware, and offensive language in emails.
- Emails from unknown sources, chain letters, and spam will be deleted without opening.

3. Training

- ICT support providers will run annual assemblies on phishing and malicious emails, covering:
    - Identifying legitimate email addresses
    - Recognising phishing addresses
    - Awareness of emails urging immediate action

    - Checking spelling and grammar as potential red flags

4. Incident Response

- Any cyber-attack or breach through email will be managed according to the **Cyber Response and Recovery Plan**.

19. Generative AI

1. Safety First

- Safety is the top priority in deciding whether to use AI tools.
- Staff and pupils may only use AI where clear benefits outweigh risks, such as reducing teacher workload.
- All AI use must comply with statutory obligations, including KCSIE (Keeping Children Safe in Education).

2. Risk Assessment and Mitigation

- The school will carry out an **AI Risk Assessment** to evaluate potential risks.
- Mitigation plans will address unauthorised or unsafe use cases.

3. Pupil Use

- Pupils may use generative AI only under supervision and with tools that include appropriate filtering and monitoring.
- Measures will be in place to prevent pupils from accessing or creating harmful or inappropriate content.

4. Compliance and Safeguarding

For any AI use, the school will:

- Comply with age restrictions set by AI tools and open-access LLMs.
- Consider online safety in all safeguarding policies.
- Follow KCSIE for statutory safeguarding obligations.
- Refer to the DfE generative AI product safety expectations, including filtering and monitoring standards.

5. Preparing Pupils for Emerging Technology

- Pupils will be educated on safe and appropriate AI use, considering their age.
- The IT system will include filters and monitoring systems to prevent harmful or inappropriate AI content.
- Personal and sensitive data must not be entered into AI tools in an identifiable form.

6. Guidance and Foundations

- The school will use existing guidance and support to ensure safe, secure, and reliable AI foundations before introducing more advanced AI technologies.

7. Safe Use of AI Policy

- The school will maintain a comprehensive Safe Use of AI Policy that:

  - Defines responsible and secure AI use.
  - Identifies potential risks of misuse.
  - Outlines safeguarding measures to ensure safe and ethical AI application.

20. Social Networking

- The use of social media by staff and pupils will be managed in accordance with the school's Social Media Policy.
- All staff and pupils are expected to follow the guidance and rules outlined in that policy when using social networking platforms, both on and off school devices.

21. School Website

- The headteacher is responsible for the overall content of the school website.
- They must ensure that the website content is appropriate, accurate, up-to-date, and meets government requirements.
- Management of the website will follow the school's Website Policy.

22. Use of Devices

- **School-owned devices** may be issued to staff and pupils to support teaching, learning, and administrative work.
- The use of **personal devices** on school premises or for school-related work will follow the Acceptable Use Agreement statements.

23. Remote Learning

- All remote learning will be delivered in accordance with the school's Remote Education Policy.
- The policy outlines how online safety is maintained during the delivery of remote education.

24. Monitoring and Review

- The school recognises the rapidly changing online environment.
- The DSL, ICT external support providers, and headteacher conduct half-termly light-touch reviews of this policy to evaluate effectiveness.
- The governing board, headteacher, and DSL conduct a full review annually and after any online safety incidents.
- **The next scheduled review is August 2026.**
- Any changes to the policy are communicated to all members of the school community.

Approved by Board of Governors August 2025