



St Mary's CE Primary School

N8 7QN

Online Safety Policy (Including Acceptable Use Guidance) 2026

Jesus said, "Love one another as I have loved you." (John 15:12)

Our Vision

As we love, we flourish

As we flourish, we aspire

As we aspire, we achieve

Together, we are a family.

Friendship, Compassion, Hope, Wisdom, Community, Endurance.

Approved by:	FGB	Date: October 2026
Last reviewed on:	October 2026	
Next review due by:	October 2027	

Through our daily school life at St Mary's Church of England Primary School we encourage our children to build respectful friendships and demonstrate compassion towards others. Through this we build a strong community spirit, as together we are a family. Our teaching and learning provides the children with the wisdom and endurance they need to expand their minds socially, morally and academically so allowing them to achieve and flourish and fulfil 'Life in all its Fullness.' (John 10:10). We encourage our children to demonstrate and develop a dignity in their work and themselves which enables them to hope to aspire to be the best they can possibly be.

E Safety and Internet Usage

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Ensure students are educated in how to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour and identify a range of ways to report concerns about content and contact.
- Establish clear mechanisms to intervene and escalate an incident, where appropriate.

E safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, **misogyny and misandry**, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as **making or sharing of nudes and semi-nudes** (including digitally altered or AI-generated images), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Links with other policies

The school's Online Safety Policy will operate in conjunction with other policies including those for Computing, Positive Behaviour, Anti-Bullying, Safeguarding and Child Protection, Data Protection and child-on-child Abuse Policy.

2. Background - Why Is Internet Use Important?

The purpose of internet use in school is to raise educational standards, to promote children achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business, and social interaction. Access to the internet is therefore an entitlement for children who show a responsible and mature approach to its use and St Mary's has a duty to provide children with quality internet access.

Many children will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

3. How Does Internet Use Benefit Education?

Benefits of using the internet in education include

- Access to world-wide educational resources including museums, libraries, and art galleries.
- Rapid and cost-effective worldwide communication.
- Inclusion in the National Education Network which connects all UK schools (LGfL).
- Educational and cultural exchanges between children worldwide.
- Access to experts in many fields for children and staff.
- Professional development for staff through access to national developments, educational materials, and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority.
- Access to learning wherever and whenever convenient.
- Greatly increased skills in literacy.
- In times of lockdowns and global pandemics, internet access allows students to continue learning remotely.

4. How Can Internet Use Enhance Learning?

- The school internet access is designed expressly for children use and includes filtering appropriate to the age of our children.
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use in line with Computing Policy and NC objectives.
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide children in online activities that will support learning outcomes planned for the children' age and maturity.
- Children will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation in line with Computing policy and NC objectives.

5. Good Habits

E safety depends on effective practice at several levels:

- Responsible ICT use by all staff and children; encouraged by education and made explicit through published policies.
- Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband from the provider including the effective management of content filtering.
- National Education Network / LGfL standards and specifications.

6. Dangers To Consider

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyberbullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy, and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Modern slavery and exploitation – the risk of children being targeted for criminal or sexual exploitation through online contact
- Financial exploitation – including online scams, fraud, and coercion to engage in financial transactions
- AI-generated harmful content – including deepfakes, digitally altered images, and synthetic media that could be used to harm, deceive, or exploit children
- Child-to-parent or caregiver abuse – where online content or behaviours contribute to or facilitate abuse directed at parents or carers

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build children's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The Online Safety Policy that follows explains how we intend to do this.

7. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping Children Safe in Education (2026)**, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary,

searching for and deleting inappropriate images or files on children's electronic devices where they believe there is a 'good reason' to do so.

Data protection compliance:

Personal data will be recorded, processed, transferred and made available according to **data protection legislation**, which collectively encompasses:

- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The Data (Use and Access) Act 2025

The policy also takes into account the National Curriculum computing programmes of study.

8. Roles and responsibilities

8.1 The governing body

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

- Identified governor to oversee online safety.
- All governors will ensure that they have read and understood this policy and will adhere to the terms of it and the acceptable use guidance for staff, governors, volunteers and visitors (Appendix 3).

8.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

8.3 The Designated Safeguarding Lead (DSL)

Details of the school's DSL are set out in our Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, computing lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged either using 'Arbour' or 'My Concern' and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Supporting the annual filtering and monitoring review in partnership with the SLT member responsible and IT support
- Overseeing the school's approach to social transition requests, ensuring compliance with KCSIE 2026 and parental partnership principles
 - Maintaining oversight of AI and generative AI risks, including reviewing approved tools and responding to AI-related incidents
 - Ensuring accurate recording of children's biological sex in safeguarding and welfare records

This list is not intended to be exhaustive.

8.4 External ICT support

We currently outsource ICT to a third-party company – Islington Help Desk.

The Senior Leadership Team member responsible for filtering and monitoring (typically the headteacher or deputy/assistant headteacher) has overall accountability for ensuring filtering and monitoring systems are effective and compliant.

The ICT manager (Islington Help Desk) is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep children safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems monthly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- **Providing technical support and data for the annual filtering and monitoring review conducted by the SLT member and DSL**
- **Implementing any changes or recommendations arising from the annual review**

This list is not intended to be exhaustive.

8.5 All staff

All staff, including contractors and agency staff, and volunteers who undertake regular activities at school will:

- Ensure that they have read and understood this policy
- Adhere to the terms of it and the acceptable use guidance for staff, governors, volunteers and visitors (Appendix 3).
- Work with the DSL to ensure that any online safety incidents are logged on using 'Arbor' or 'My Concern' as appropriate and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Staff will have regular updates and training on E-Safety requirements

This list is not intended to be exhaustive.

8.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Adhere to the terms of it and the acceptable use guidance for parents and carers (Appendix 1 or 2 depending on the Key Stage their child is in).
- Ensure their child is aware of and adheres to the terms of this policy and the acceptable use guidance for children (Appendix 1 or 2 depending on the Key Stage their child is in).
- Parents should consult the E-Safety section of the school website, which gives further guidance on keeping children safe online, and giving links to several useful organisations.
- Parents' attention will be drawn to the E-safety Policy and expectations/guidance in newsletters, communication home and on the school website.
- Parents will receive a copy of their child's Acceptable Use Agreement.

8.7 Visitors and members of the community

All visitors to the school will, where appropriate:

- Be made aware of this policy via our school website, and, if appropriate, be given a copy of the acceptable use guidance for staff, governors, volunteers and visitors (Appendix 3).

8.8 Children

- Children will be made aware of the acceptable use guidance for children (Appendix 1 and 2) during lessons, assemblies and workshops.
- Rules for internet access will be posted in all classrooms.
- Children will be informed that internet use will be monitored.
- Children will be reminded of E safety rules regularly – especially when using the internet.

9 Email & Online Collaboration

- Children may only use approved email accounts on the school system.
- LGfL USO accounts have been created for each child at St Mary's Primary with enhanced safeguarding measures in place to ensure our children's safety as much as possible.
- Children must immediately tell a teacher if they receive offensive messages.
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Children must not access others children's accounts or files.
- Whole class or group email addresses should be used in school.
- Children must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Children must not deliberately seek out offensive materials. Should any children encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site.
- Children are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- Children must ask permission before accessing the internet and have a clear idea of why they are using it.
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- No program files may be downloaded from the internet to the computer, to prevent corruption of data and to avoid viruses.
- Children must not bring in USBs from home for use in school without permission. This is for both legal and security reasons. USB ports are disabled in school.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain letters is not permitted.
- Children must sign an agreement form if using school device at home which includes a code of conduct.

10 Social Networking

- At St Marys we block/filter access to social networking sites and newsgroups unless a specific use is approved.

- Children are advised never to give out personal details of any kind which may identify them or their location.
- Children are advised not to place personal photos on any social network space.
- Children are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Children are encouraged to invite known friends only and deny access to others
- Children and parents are made aware that some social networks are not appropriate for children of primary school age and that the legal age to hold accounts on many, such as YouTube or Instagram, is 13 years old.

It is possible that a high proportion of staff will have their own social networking site accounts. They should protect their professional reputation by using their personal accounts appropriately.

Guidelines are issued to staff:

- Staff must **never** add children as 'friends' into their personal accounts (including past children under the age of 16).
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts.
- Staff **must not** post comments about the school, children, parents or colleagues including members of the governing body.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should use social networking only in ways that do not conflict with the current national teacher's standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action

11 Filtering

The school will work in partnership with Islington Help Desk and LGfL, our I.T. support provider and internet Service Provider respectively, to ensure filtering systems are as effective as possible. The school regularly reviews its filtering and monitoring systems to ensure they meet the standards set out in the DfE's guidance, and it has appropriate processes for reporting and responding to concerns identified through monitoring.

11A. Filtering and Monitoring: Annual Review Process

Statutory Requirement:

The school must conduct a strict review of its filtering and monitoring systems **at least once every academic year**. This is a mandatory requirement under KCSIE 2026.

Review Responsibilities:

The annual review must be conducted by:

- The **Senior Leadership Team (SLT) member** responsible for filtering and monitoring (typically the headteacher or deputy headteacher)
- Supported by the **Designated Safeguarding Lead (DSL)**
- With input from **IT support** (Islington Help Desk)

Review Process:

The annual review will assess:

- 1. Effectiveness of filtering systems:**
 - Whether inappropriate content is being successfully blocked
 - Any instances where legitimate educational content has been over-blocked
 - Updates needed to filtering categories and policies
 - Compliance with DfE filtering standards
- 2. Effectiveness of monitoring systems:**
 - Whether concerning online activity is being identified and flagged
 - Response times to alerts and incidents
 - Staff awareness and understanding of monitoring reports
 - Privacy and proportionality of monitoring
- 3. Incident analysis:**
 - Review of all online safety incidents from the past year
 - Patterns or trends requiring policy or system changes
 - Effectiveness of responses to incidents
- 4. System updates and maintenance:**
 - Whether systems are up to date with latest software and threat definitions
 - Any technical issues or vulnerabilities identified
 - Recommendations from IT support provider

Documentation:

The SLT member responsible will produce a written report documenting:

- Date of review and participants
- Findings and assessment of current systems
- Any incidents or concerns identified
- Actions taken or recommended
- Date of next scheduled review

This report will be presented to the governing body and retained as evidence of compliance.

12 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Please see our Data Protection policy.

13 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the E safety policy is adequate and that the implementation of the E safety policy is appropriate.

14 Handling E safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Children and parents will be informed of the complaints procedure.

15 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and their risks assessed.

16 Use of Communication and Information Technology In School (Mobile Phones)

School policy on mobile phone-free environment:

In line with KCSIE 2026 guidance, St Mary's CE Primary School operates as a **mobile phone-free environment**. This means that pupil access to mobile phones is restricted during lessons, break times, and lunchtimes to:

- Minimise distractions and support learning
- Reduce online safety risks during the school day
- Promote face-to-face social interaction
- Prevent incidents involving inappropriate content or cyber-bullying

Limited exception for independent travellers:

Only Y5 and Y6 children who are independent travellers to and from school are allowed to bring their phones to school under the following strict conditions:

- These phones must be dumb or brick phones, not smartphones and must not be used during the school day.
- They must be handed to the teacher for safekeeping throughout the day and returned to the child at the end of the day.

17 When using email, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email or electronic message that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and parents must be professional in tone and content
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and reminded to write emails clearly and correctly, without including any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

18 Educating children about online safety

Children will be taught about online safety as part of the curriculum:

In **Key Stage 1**, children will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Children in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, children will know:

- *That people sometimes behave differently online, including by pretending to be someone they are not*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*
- The safe use of social media and the internet will also be covered in other subjects where relevant.

19 Educating parents about online safety

- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
- Online safety will also be covered during parents' evenings.
- As part of Safer Internet Day, an E-safety talk will be held, raising awareness and offering advice or support.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

20. Shared Safeguarding Duties: Third-Party Providers

The school recognises that it shares active safeguarding duties regarding all adults who work with our pupils, including:

- Supply teachers
- Trainee teachers on placement
- Contracted staff (e.g., sports coaches, music teachers, IT support)
- Volunteers

Before any third-party provider works with pupils:

The school will:

- Ensure appropriate safer recruitment checks have been completed
- Provide them with a copy of this Online Safety Policy
- Ensure they understand and agree to the acceptable use guidance (Appendix 3)
- Brief them on reporting procedures for online safety concerns
- Confirm they understand their safeguarding responsibilities

Ongoing responsibilities:

- Third-party providers must adhere to the same online safety standards as school staff
- They must report any online safety concerns to the DSL immediately
- The school will monitor their compliance with this policy
- Any breaches will be addressed through the relevant contract or placement agreement

21. Temporary Accommodation Notification Duty

The school is aware of the **temporary accommodation notification duty** placed on local housing authorities when relocating children.

What this means for the school:

When a local housing authority places a family with school-age children in temporary accommodation in our area, they have a duty to notify:

- The local authority where the temporary accommodation is located
- Relevant services, including schools

The school's responsibilities:

- We will work collaboratively with the local housing authority and children's social care when notified of children placed in temporary accommodation
- We recognise that children in temporary accommodation may be particularly vulnerable and may face additional safeguarding risks, including online safety risks
- We will ensure these children receive appropriate support and monitoring
- The DSL will be informed of any such placements and will consider whether additional safeguarding measures are needed

22. Single-Sex Sports and Facilities: Safeguarding Requirements

Statutory requirement:

KCSIE 2026 introduces mandatory restrictions regarding facilities and activities designated for a specific biological sex.

22.1 Facilities Usage

Children are **prohibited from entering** the following facilities designated for the opposite biological sex:

- Toilets
- Changing rooms
- Boarding or residential accommodation (where applicable)

There are no exceptions to this requirement, including when supporting a child's social transition.

Implementation:

- All facilities will be clearly designated by biological sex
- Staff will ensure children use facilities appropriate to their biological sex
- Any concerns or requests from pupils or parents will be referred to the headteacher and DSL
- The school will consider reasonable adjustments where appropriate (e.g., provision of private facilities) but will not permit use of facilities designated for the opposite biological sex

22.2 Physical Education and Sports

Children are prohibited from participating in PE classes or sports designated for the opposite biological sex.

Rationale:

The school recognises that separating children into sports based on biological sex is:

- Legally permitted for reasons of safety and fairness
- Does not violate non-discrimination laws
- Protects the welfare and safety of all pupils
-

Implementation:

- PE and sports activities may be organised by biological sex where appropriate for safety and fairness
- Decisions will be made on a case-by-case basis considering the nature of the activity, age of pupils, and safety considerations
- Any concerns will be addressed through consultation with parents, the DSL, and senior leadership

22.3 Recording of Biological Sex

The school is legally required to record a child's biological sex accurately wherever it is recorded, including:

- Admissions records
- Management information systems
- Registers
- Safeguarding records
- Medical records

Staff must ensure biological sex is recorded correctly and must not alter records to reflect a social transition.

23. Making or Sharing of Nudes or Semi-Nudes

23.1 Definition and Scope

The making or sharing of nudes or semi-nudes refers to the creation, possession, or distribution of nude or semi-nude images, videos, or livestreams involving children. This includes both consensual and non-consensual incidents.

This encompasses:

- **Original images or videos** – photographs or recordings created using cameras, smartphones, or other devices
- **Digitally altered images** – photographs or videos that have been manipulated, edited, or modified using software or applications
- **AI-generated content** – images or videos wholly or partially created using artificial intelligence, including deepfakes and other synthetic media that depicts children in nude or semi-nude form

The making or sharing of nudes or semi-nudes counts as unacceptable use of ICT and internet, regardless of how the content was created or whether it involves real, altered, or artificially generated imagery.

23.2 Mandatory Safeguarding Response

All incidents involving the making or sharing of nudes or semi-nudes mandate a safeguarding response.

The school will treat every incident as a serious safeguarding issue, whether the content involves:

- Real photographs or videos of children
- Digitally altered images of real children
- Wholly AI-generated images that appear to depict children
- Content shared consensually between peers
- Content shared non-consensually or maliciously

There are no exceptions to this requirement. Even if an incident appears minor or consensual, it must be reported to the Designated Safeguarding Lead (DSL) and handled through safeguarding procedures.

23.3 Reporting and Response Procedures

Immediate actions when an incident is discovered or reported:

1. **Do not view, forward, or share the content** – this may constitute a further offence
2. **Confiscate the device(s) involved** in line with the school's powers under the Education and Inspections Act 2006 and Education Act 2011
3. **Report immediately to the DSL** – do not delay or attempt to investigate independently
4. **Preserve evidence** – ensure devices are not tampered with and record details of the incident

The DSL will:

- Assess the incident using the school's safeguarding procedures and risk assessment framework
- Consider the context, including:
 - The age and vulnerability of all children involved
 - Whether the content was created, altered, or generated, and by whom
 - Whether the sharing was consensual or non-consensual
 - Whether there are any aggravating factors (e.g., coercion, malicious intent, wider distribution)
 - Whether adults are involved or there are concerns about grooming or exploitation
- Determine appropriate next steps, which may include:
 - Referral to children's social care
 - Referral to the police (mandatory for certain circumstances, including suspected criminal offences)
 - Involvement of parents/carers (unless this would increase risk to the child)
 - Support for affected children, including pastoral care and counselling
 - Disciplinary action in line with the school's behaviour policy
 - Review of online safety education and preventative measures

Referral to police:

The DSL will refer incidents to the police where:

- The content involves sexual acts or poses that are indecent
- There is evidence of adult involvement or grooming
- There is evidence of coercion, blackmail, or exploitation
- The content has been shared widely or published online
- There are aggravating factors such as malicious intent or significant harm
- The incident involves AI-generated content that may constitute an offence under relevant legislation

The school recognises that creating, possessing, or distributing indecent images of children is a criminal offence, even if the images are created by children themselves or generated using AI.

23.4 Education and Prevention

The school will educate children about the risks and consequences of making or sharing nudes or semi-nudes through:

- **Age-appropriate online safety education** as part of the computing curriculum, PSHE, and RSE

- **Specific teaching about:**
 - Why creating, sharing, or possessing such content is harmful and illegal
 - The permanence of digital content and how quickly it can spread
 - The emotional and psychological impact on victims
 - The risks of coercion, pressure, and exploitation
 - How AI tools can be misused to create harmful content, including deepfakes
 - How to recognise and resist pressure to create or share such content
 - How to report concerns and seek help from trusted adults
 - The legal consequences for children and young people involved in such incidents
- **Regular reminders and reinforcement** through assemblies, online safety lessons, and Safer Internet Day activities
- **Clear messaging** that the school's response is focused on safeguarding and support, not punishment, to encourage reporting

23.5 Support for Affected Children

Children involved in incidents (whether as victims, perpetrators, or both) will receive appropriate support, which may include:

- Immediate pastoral support and reassurance
- Access to counselling or therapeutic services
- Safety planning to prevent further harm or distribution of content
- Education about healthy relationships, consent, and online safety
- Ongoing monitoring and support as part of a safeguarding plan
- Liaison with external agencies where appropriate

The school recognises that children involved in making or sharing nudes or semi-nudes may themselves be victims of exploitation, coercion, or abuse, and will ensure that responses are trauma-informed and child-centred.

23.6 Staff Training

All staff will receive training on:

- Recognising and responding to incidents involving nudes or semi-nudes
- Understanding that AI-generated and digitally altered content is included in this category
- The mandatory requirement for a safeguarding response to all incidents
- Procedures for reporting to the DSL
- The importance of not viewing, forwarding, or sharing content
- How to support affected children

This training will be included in safeguarding induction for new staff and refreshed annually for all staff.

24. Staff using work devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use guidance, as set out in Appendix 3.
- Work devices must be used solely for work activities
- If staff have any concerns over the security of their device, they must seek advice from the computing lead or ICT Manager (Islington Help Desk).

25. How the school will respond to issues of misuse

- Where a children misuses the school's ICT systems or internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

26. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including:

- Cyber-bullying and the risks of online radicalisation
- **Making or sharing of nudes or semi-nudes**, including AI-generated and digitally altered content
- **AI and generative AI risks and appropriate use**
- **Social transition: the school's approach and parental partnership requirements**
- **Filtering and monitoring systems and how to report concerns**

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, staff meetings, and briefings on emerging risks).

Specific training topics will include:

- Updated terminology and definitions (e.g., "making or sharing of nudes or semi-nudes")
- Recognising and responding to AI-related risks
- Understanding the mandatory safeguarding response to all incidents involving nudes or semi-nudes
- The school's approach to social transition and facilities usage
- Annual filtering and monitoring review findings and any changes to systems

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training, **including understanding their oversight role in the annual filtering and monitoring review.**

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

27: Artificial Intelligence and Generative AI

27.1 Scope and Purpose

St Mary's CE Primary School recognises that Artificial Intelligence (AI) and Generative AI tools present both significant educational opportunities and safeguarding risks. This section sets out how the school will assess and manage these risks to protect children, staff, and data while enabling responsible innovation in teaching and learning.

27.2 Risk Assessment and Management

The school will assess and manage risks associated with AI tools through the following framework:

Before introducing any AI tool, the school will:

- Conduct a safeguarding risk assessment considering content generation, data privacy, age-appropriateness, and potential for misuse
- Evaluate data protection implications, ensuring compliance with the Data Protection Act 2018, UK GDPR, and Data (Use and Access) Act 2025
- Review the tool's terms of service, privacy policy, and age restrictions
- Assess whether the tool processes personal data and, if so, ensure appropriate data processing agreements are in place
- Consider ethical implications, including bias, accuracy of information, and environmental impact
- Obtain approval from the headteacher and DSL before deployment

Ongoing risk management includes:

- Regular monitoring of AI tool usage by staff and pupils
- Annual review of all approved AI tools as part of the filtering and monitoring review process
- Immediate suspension of any tool if safeguarding concerns arise
- Maintaining a register of approved AI tools, accessible to all staff

27.3 Staff Guidance on Appropriate Use of AI in Teaching

Permitted uses: Staff may use AI tools for educational purposes where:

- The tool has been formally approved by the headteacher and DSL
- Use aligns with curriculum objectives and enhances learning outcomes
- Appropriate supervision and safeguards are in place
- Children are educated about the tool's capabilities and limitations

Examples of appropriate use include:

- Generating differentiated learning materials or lesson ideas (subject to teacher review and editing)
- Creating visual aids or illustrations for teaching
- Supporting pupils with additional needs (e.g., text-to-speech, translation tools)
- Demonstrating critical thinking skills by analysing AI-generated content for accuracy

Prohibited uses: Staff must not use AI tools to:

- Process children's personal data without explicit approval and appropriate safeguards
- Generate content that could be harmful, inappropriate, or discriminatory
- Replace professional judgment in assessment, safeguarding decisions, or pastoral care
- Create or share images of children (real or AI-generated)
- Automate communications with parents without human oversight

Professional responsibilities:

- Staff must verify the accuracy of AI-generated content before using it with pupils
- Staff must not present AI-generated content as their own original work
- Staff must model critical evaluation of AI outputs and teach pupils to do the same
- Staff must report any concerning AI-generated content to the DSL immediately
- Staff must maintain professional standards when using AI tools, as set out in Appendix 3

27.4 Pupil Education About AI-Generated Content

The school will educate pupils about AI and AI-generated content through:

Key Stage 1:

- Age-appropriate introduction to the concept that computers can create pictures, text, and sounds
- Teaching that not everything online is created by real people
- Encouraging pupils to ask a trusted adult if they're unsure about content they encounter

Key Stage 2:

- Understanding what AI is and how it works at a basic level
- Recognising that AI can generate realistic-looking images, videos (including deepfakes), and text
- Developing critical thinking skills to question the source and accuracy of online content
- Understanding that AI-generated content can contain errors, bias, or inappropriate material
- Learning about the risks of AI-generated content, including:
 - Deepfakes and digitally altered images that can be used to deceive or harm
 - AI-generated misinformation and "fake news"
 - Inappropriate content that AI tools might generate
- Knowing how to report concerns about AI-generated content to a trusted adult
- Understanding the ethical implications of creating and sharing AI-generated content

By the end of primary school, pupils will know:

- That AI tools can create realistic content (text, images, videos) that may not be accurate or truthful
- How to critically evaluate online content, including questioning whether it might be AI-generated
- That creating or sharing harmful AI-generated content (including deepfakes of real people) is unacceptable and may be illegal
- How to report concerns about AI-generated content they encounter

Curriculum integration: AI literacy will be taught through:

- Computing curriculum (understanding how AI works, creating simple AI projects)
- PSHE and RSE (online safety, critical thinking, digital citizenship)
- Cross-curricular opportunities (evaluating sources in research, media literacy)
- Dedicated online safety lessons and assemblies
- Safer Internet Day activities

27.5 Reporting and Responding to AI-Related Concerns

Pupils and staff must report immediately if they:

- Encounter AI-generated content that is harmful, inappropriate, or concerning
- Discover deepfakes or digitally altered images of children or staff
- Become aware of AI tools being used to create inappropriate content
- Have concerns about data privacy in relation to AI tool use

The school will respond by:

- Treating all reports seriously and investigating promptly
- Involving the DSL in all safeguarding-related AI incidents
- Preserving evidence where appropriate (screenshots, URLs, etc.)
- Taking appropriate action, which may include:
 - Blocking access to problematic AI tools
 - Reporting to relevant authorities (police, CEOP, platform providers)
 - Providing support to affected pupils or staff
 - Reviewing and updating risk assessments and policies

27.6 Review and Development

Given the rapidly evolving nature of AI technology:

- This section will be reviewed at least annually as part of the Online Safety Policy review
- The school will stay informed about emerging AI risks and guidance through:
 - DfE updates and statutory guidance
 - Professional networks and training
 - Collaboration with our IT support provider (Islington Help Desk)
 - Safeguarding partnerships and local authority guidance
- Staff will receive regular training updates on AI-related safeguarding risks
- The approved AI tools register will be reviewed termly

28.Social Transition: Safeguarding Approach

28.1 Definition

Social transition refers to a child adopting the name, pronouns, appearance, or other social markers associated with a gender different from their biological sex.

28.2 School's Approach

The school must not initiate any action regarding social transition. We will only respond if a child or their parent specifically requests support.

28.3 Parental Partnership

The school will work in partnership with parents regarding any requests related to social transition. This means:

- **Parents must be involved in all decisions** relating to their child's social transition
- Staff must not adopt any changes relating to social transition (e.g., name, pronouns, use of facilities) without a decision involving the parents
- The school will facilitate open, respectful dialogue between parents and their child where appropriate

25.4 Exceptional Circumstances

The only exception to parental involvement is in **exceptionally rare cases** where involving parents would pose a **greater risk to the child**.

In such cases:

- The DSL must be involved in the decision
- A full risk assessment must be conducted
- The decision must be documented with clear rationale
- Advice from children's social care or other relevant agencies must be sought
- The decision will be reviewed regularly

25.5 Primary School: Particular Caution

As a primary school, we will exercise **particular caution** regarding social transition.

Full social transition in primary school should be agreed very rarely. Any such decision will involve:

- Extensive consultation with parents
- Input from the DSL and headteacher
- Consideration of the child's age, maturity, and understanding
- Assessment of potential risks and benefits
- Ongoing review and support

28.6 Staff Responsibilities

All staff must:

- Refer any requests or questions about social transition to the headteacher and DSL immediately
- Not make any changes to how they address or treat a child without senior leadership approval
- Maintain accurate records using the child's legal name and biological sex
- Treat all children with respect and dignity regardless of how they present or identify
- Understand that supporting a child's wellbeing does not require agreeing to social transition

28.7 Recording and Facilities

As outlined in Section 22:

- The school must record biological sex accurately in all records
- Children must use facilities (toilets, changing rooms) designated for their biological sex
- Children must participate in PE/sports designated for their biological sex
- These requirements apply regardless of any social transition

This Online Safety Policy is fully compliant with Keeping Children Safe in Education (KCSIE) 2026 and reflects all statutory requirements effective from September 2026, including:

- Updated terminology for making or sharing of nudes or semi-nudes
- Mandatory safeguarding response to all such incidents
- Explicit inclusion of AI-generated and digitally altered content
- Annual filtering and monitoring review process with designated SLT responsibility
- Updated data protection legislation references
- Mobile phone-free environment policy
- Single-sex facilities and sports requirements
- Social transition approach with parental partnership
- Shared safeguarding duties for third-party providers
- Recognition of modern slavery, financial exploitation, and emerging risks

Appendix 1: EYFS and KS1 acceptable use guidance - children and parents/carers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: GUIDANCE FOR CHILDREN AND PARENTS/CARERS

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I am aware that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 2: KS2 - acceptable use guidance for children and parents/carers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: GUIDANCE FOR CHILDREN AND PARENTS/CARERS

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission.
- I will hand my phone in to my class teacher at the beginning of the day and it will be locked away by the teacher until home time
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I know that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 3: acceptable use guidance for staff, governors, volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: GUIDANCE FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Not take photographs of children without checking that they can be photographed.
- Not take photographs of children using my mobile phone or personal devices.
- Share confidential information about the school, its children or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will:

- Only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- Take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- Let the designated safeguarding lead (DSL) and ICT manager know if a children informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- Always use the school's ICT systems and internet responsibly, and ensure that children in my care do so too.

I know:

- That the school will monitor the websites I visit and my use of the school's ICT facilities and systems.