Online Safety, Acceptable Use, and Digital Technology Policy

St Joseph’s Catholic Primary School

Approved by:

Last reviewed on:

Next review due by:

Contents

1. Policy Statement, Rationale, and Aims

At St. Joseph's Catholic Primary School, we recognise that all children have rights as outlined in the UN Convention on the Rights of the Child (UNCRC). As duty bearers, we have the responsibility to respect, protect, and fulfil these rights, ensuring that all our children grow and learn as rights-holders. This policy directly supports the following Articles of the UNCRC:

- **Article 13** – The right to find out things and share thoughts freely, through words, writing, or drawing, unless it harms or offends others.
- **Article 17** – The right to access reliable information from the media and the responsibility of adults to ensure that this information is not harmful and is understood.
- **Article 19** – The right to be protected from all forms of harm, including abuse and mistreatment.

We believe that the Internet and digital technologies are powerful tools that, when used appropriately, can enrich education, enhance communication, and promote learning across all areas of the curriculum. At the same time, we acknowledge that, without clear guidance and safeguards, technology can expose children to risks such as misinformation, harmful content, and inappropriate contact.

Our commitment is to create a safe digital environment by:

- Educating children to be discerning, respectful, and responsible users of technology.
- Empowering staff and parents with the knowledge and tools to guide children’s safe use of the Internet.
- Promoting the use of technology in a way that upholds children’s rights, well-being, and development.

This policy outlines our approach to online safety and sets out the responsibilities of pupils, staff, parents, and governors in keeping our school community safe online. It is reviewed annually to reflect the latest guidance, legislation, and technological developments.

1.1 Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others. Particularly vulnerable groups include children with SEND, young carers, children looked after, and children who may be more susceptible to online grooming or radicalization.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (referred to as ‘mobile phones’).
- Establish clear mechanisms to identify, intervene, and escalate an incident, where appropriate.

1.2 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, self-harm, suicide, antisemitism, 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, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images, and online bullying.
- **Commerce** – Risks such as online gambling, inappropriate advertising, phishing, and/or financial scams.

2. Legislation, Guidance, and Legal Framework

This policy is informed by both statutory and non-statutory legislation and guidance that ensures the safety, rights, and wellbeing of children in the digital space. It is aligned with key safeguarding and educational frameworks to provide a comprehensive approach to online safety.

2.1 Key Legislation and Guidance:

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, **Keeping Children Safe in Education (KCSIE) 2024**, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: Advice for headteachers and school staff
- Searching, screening, and confiscation

Furthermore, this policy aligns with the whole-school safeguarding approach outlined in **KCSIE 2024**, which includes mental health considerations and embedding online safety across the wider curriculum. The policy also refers to:

- DfE guidance on protecting children from radicalisation
- The National Curriculum computing programmes of study
- Legislation including (but not limited to):
    - **The Education Act 1996** (as amended)
    - **The Education and Inspections Act 2006**
    - **The Equality Act 2010**
    - **The Education Act 2011**, which empowers teachers to search for and delete inappropriate material from pupils' devices if there is 'good reason' to do so.

Additionally, this policy reflects:

- Updates from **Working Together to Safeguard Children (2023)**
- The developing implications of the **Online Safety Act 2023/24**, which introduces a legal duty of care on digital platforms to protect children from harmful online content.
- The **DfE Filtering and Monitoring Standards (2024)**, which require schools to:
    - Assign clear roles and responsibilities for managing filtering and monitoring
    - Review filtering and monitoring systems at least annually
    - Ensure safeguarding is not compromised by overly restrictive measures that hinder teaching and learning
    - Log and act upon any failures or breaches in filtering and monitoring systems

2.2 Legal Framework:

This policy is also guided by the following key pieces of legislation and guidelines that further ensure the safety and rights of children in the digital space:

- **The UN Convention on the Rights of the Child (UNCRC)**: Articles 13, 17, and 19 emphasise the rights of children to access information, share ideas, and be protected from harm.
- **The Children's Act 1989**: Establishes the duty of care that schools have to protect children from harm, extending to their online safety.
- **The Education and Training (Welfare) Act 2020**: Provides a framework for safe and appropriate use of digital technology in schools.
- **The Data Protection Act 2018 and GDPR**: Ensures the protection of children's personal data when using the internet and safeguards data when interacting online or using school resources.
- **The UK Safer Internet Centre and the DfE**: Provide online safety guidelines for schools, including addressing issues such as cyberbullying, child protection, and safe communication in the digital world.
- **The Prevent Duty (Counter-Terrorism and Security Act 2015)**: Requires schools to have due regard to preventing children from being drawn into terrorism, which includes preventing access to harmful online content.

- **Online Safety Bill 2025**: Sets provisions for the protection of children from harmful content, including stricter controls over user-generated content and the responsibilities of social media platforms and digital companies.

These legal frameworks ensure that the safety, rights, and education of children in our school community are upheld, creating a safe online environment where technology is used to enhance learning and development.

2.3 Data Protection and Security:

GDPR Compliance: All personal data is processed in accordance with the **Data Protection Act 2018** and **GDPR** guidelines. Digital images and data are stored securely, with access restricted to authorized staff only.

2.4 Maintaining the Security of the ICT Network:

Virus Protection and Security Updates: All school computers receive regular updates with virus protection software. Staff are encouraged to keep their devices up-to-date with the latest security software to protect against potential cyber threats.

2.5 Physical Environment / Security

• The school strives to provide a secure environment for the whole community, regularly reviewing physical and network security.
• Anti-virus software is installed on all computers and updated regularly.
• Central filtering is provided and managed by the MAC IT team.
• If an inappropriate site is discovered, it must be reported to the Online Safety co-ordinator, who will report it to the IT team to be blocked. All incidents will be recorded in the Online Safety log for audit purposes.

2.6 Scope:

This policy applies to:

- All fixed and mobile technologies that are owned, operated, and supplied by St. Joseph’s Catholic Primary School.
- Personal devices (e.g., smartphones, tablets, laptops) owned by staff, pupils, and visitors while on the school premises.
- The use of the Internet both in school and at home, when it is in connection with the school’s activities, including remote learning and homework assignments.

The policy also extends to the safe use of digital technologies for communication between staff, pupils, and parents, including email, online platforms, and social media channels where relevant.

3. Roles and Responsibilities

This section outlines the key roles and responsibilities involved in managing online safety within the school, detailing who is responsible for implementing, reviewing, and ensuring the effective operation of the online safety policy.

3.1 The Governing Board

The governing board holds overall responsibility for monitoring this policy and holding the Executive Principal and Head of School to account for its implementation.

Key responsibilities include:

- Conducting regular meetings with the Head of School to ensure online safety risks are assessed and mitigated, and appropriate systems are in place.
- Ensuring that online safety is an embedded and interrelated theme across all safeguarding policies, procedures, and practices.
- Ensuring all staff receive regular and up-to-date training on online safety as part of safeguarding and child protection, including:

    - Induction training
    - Annual refresher sessions
    - Ongoing updates via emails, bulletins, and staff meetings
- Coordinating regular meetings with relevant staff to review:
    - Online safety concerns
    - Training needs
    - Reports and logs maintained by the Designated Safeguarding Lead (DSL)
- Ensuring children are taught how to stay safe online, including vulnerable groups such as those with special educational needs and/or disabilities (SEND), and victims of abuse. The board will ensure teaching is adapted where necessary, avoiding a one-size-fits-all approach.
- Ensuring the school implements filtering and monitoring systems that:
    - Are reviewed at least annually
    - Are effective in blocking harmful/inappropriate content without unnecessarily disrupting teaching and learning
    - Meet DfE filtering and monitoring standards
    - Have clear roles and responsibilities assigned for management
    - Are supported through collaboration with IT staff and service providers

All governors are expected to:

- Read and understand this policy
- Agree to and follow the terms outlined in the acceptable use of the school’s ICT systems and internet
- Ensure safeguarding measures related to online safety are appropriate, contextualised, and inclusive

3.2 The Executive Principal

The Executive Principal is responsible for the consistent implementation of this policy throughout the school. Responsibilities include:

- Ensuring that all staff understand and adhere to this policy
- Collaborating with the governing board and DSL to review and update the policy annually
- Supporting the DSL and ICT Manager in addressing online safety issues and ensuring effective systems are in place

3.3 The Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for online safety in the school. This includes:

- Supporting the Executive Principal in ensuring consistent implementation of the policy
- Collaborating with the governing board, ICT Manager, and other relevant staff to review and update the policy and procedures
- Taking lead responsibility for understanding, overseeing, and managing the school's filtering and monitoring systems and processes
- Managing all online safety incidents, including cyberbullying, in line with safeguarding and behaviour policies
- Ensuring all incidents are logged appropriately
- Coordinating and delivering staff training on online safety, including using a training self-audit (see Appendix 4)
- Liaising with external agencies, including the local authority, police, and mental health services where necessary

- Conducting and reviewing annual online safety risk assessments
- Providing regular safeguarding and child protection updates, including online safety, at least annually
- Reporting regularly to the Executive Principal and governing board on online safety matters and incident trends

3.4 The ICT Manager

The ICT Manager is responsible for ensuring that the school's ICT infrastructure is secure, compliant, and supportive of online safety measures. This includes:

- Implementing and reviewing filtering and monitoring systems on school devices and networks at least annually
- Ensuring systems effectively block harmful or inappropriate content, including terrorist/extremist material, without adversely affecting educational use
- Ensuring ICT systems are secure from viruses, malware, and cyber threats, with mechanisms updated regularly
- Conducting regular security checks and audits of ICT systems
- Blocking access to unsafe or inappropriate sites and restricting potentially dangerous downloads
- Collaborating with the DSL and Executive Principal to log and manage online safety incidents in accordance with this policy and the behaviour policy

3.5 All Staff and Volunteers

All staff (including contractors, agency staff, and volunteers) have a responsibility to:

- Maintain awareness and understanding of this policy
- Implement the policy consistently and report any breaches
- Adhere to the acceptable use terms for school ICT systems and internet (see Appendix 3)
- Ensure pupils follow the school's acceptable use terms (see Appendices 1 and 2)
- Know that the DSL is responsible for the school's filtering and monitoring systems and how to report any related incidents
- Collaborate with the DSL to log and manage any incidents appropriately
- Respond to incidents of cyberbullying in accordance with the behaviour policy
- Take all reports and concerns related to online sexual violence or harassment seriously, whether they occur online or offline, maintaining the attitude of 'it could happen here'

3.6 Parents and Carers

Parents and carers are expected to:

- Ensure their child understands and agrees to the school's acceptable use terms for ICT systems and internet use
- Notify the school of any concerns or questions related to online safety
- Support the school's efforts in teaching children how to stay safe online

Additional online safety support is available through external organisations such as:

- **UK Safer Internet Centre – What are the issues?**
- **Childnet International – Hot Topics**
- **Childnet International – Parent resource sheet**

3.7 Visitors and Members of the Community

Visitors and community members who use the school's ICT systems or internet access will be:

- Made aware of this policy where relevant

- Expected to follow its terms
- Required to agree to the school’s acceptable use guidelines if applicable

4. Educational Use of the Internet

The school’s internet access is designed specifically for pupil use and includes age-appropriate filtering to protect children from harmful or inappropriate content. The internet will be used to enrich and extend learning activities, providing pupils with access to a wide range of resources such as virtual museums, interactive platforms, and educational websites.

4.1 How Will Internet Use Enhance Learning?

- **Support for Learning Objectives**: Clear objectives for internet use will be set, ensuring that online activities are aligned with specific curriculum outcomes and support both independent learning and curriculum delivery.
- **Skill Development**: Pupils will develop key skills for research, knowledge retrieval, and critical analysis through the use of online resources. These skills will be integrated into various subjects, allowing pupils to engage with content in new and meaningful ways.
- **Safe and Structured Use**: Pupils will be educated on what is acceptable and not acceptable in their internet use, ensuring they understand the boundaries of digital communication and conduct.

4.2 How Does the Internet Benefit Education?

The integration of internet technologies in education provides numerous advantages, including:

- **Access to Global Educational Resources**: Pupils can interact with digital collections from museums, art galleries, and other educational institutions worldwide, enhancing their learning experience.
- **Educational and Cultural Exchanges**: The internet facilitates virtual exchanges with schools, experts, and peers globally, broadening pupils' perspectives and fostering a global mindset.
- **Access to Experts**: Students and staff will be able to communicate directly with specialists in various fields to enrich learning and bring real-world insights into the classroom.
- **Professional Development**: Staff will have access to continuous professional development resources, educational research, and curriculum development materials to improve teaching practice.
- **Enhanced Communication**: The internet allows communication with support services, professional networks, and other educational stakeholders, fostering collaboration.

4.3 Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

In Key Stage 1 (KS1), pupils 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

Pupils in Key Stage 2 (KS2) 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, pupils 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- Understand the importance of online privacy, how their personal data is used, and the potential mental health impacts of online behaviour, including social media use

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.4 Safe Internet Usage and Training

- **Modelling Appropriate Use**: School staff will model appropriate use of the school's resources, including the internet, to promote safe online practices.
- **Testing and Filtering**: All internet activities, including homework and research, are filtered to minimize exposure to inappropriate content. Staff will ensure that links provided to students are safe and appropriate.
- **Safe Searching**: Pupils are taught how to conduct safe searches on the internet as part of their Online Safety curriculum. Resources are also provided to parents for use at home, promoting safe online habits outside of school.
- **Classroom Management**: Teachers are responsible for managing classroom activities during ICT lessons, reminding pupils of the Acceptable Use Policy before engaging in any online activities.

5. Publicising Online Safety and Parental Involvement

5.1 Effective Communication and Publicising Online Safety:

Effective communication across the school community is crucial for promoting safe and responsible digital citizenship. To ensure that all stakeholders are well-informed about the expectations and protocols surrounding online safety, we will adopt a comprehensive strategy for publicizing the Online Safety Policy and related documents, as well as engaging parents in supporting safe internet use at home.

To ensure the policy and related documents are accessible to all stakeholders, we will:

- Make the Online Safety Policy and related documents available on the school website at www.stjosutton.net.
- Introduce the policy and its related documents to all stakeholders (staff, parents, pupils, governors) at appropriate times, ensuring everyone understands their role in maintaining online safety.
- Display relevant Online Safety information in all areas where computers are used throughout the school.
- Provide ongoing Online Safety updates and information to parents through the website and regular school newsletters.

5.2 Engaging Parents in Online Safety:

The school recognizes the vital role parents play in supporting online safety at home. To engage parents and raise awareness, we will:

- Share the school’s internet policy with parents through newsletters, the school prospectus, and the school website, ensuring they are informed about expectations for safe online behaviour.
- Encourage a partnership approach with parents by offering workshops, practical sessions, and tips on promoting safe internet use at home. These will provide parents with tools to guide their children in using the internet responsibly and safely.
- Keep parents informed about the systems the school uses to filter and monitor online use.
- Inform parents about what their children are being asked to do online, including the sites they will be accessing and who from the school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns regarding online safety, these should be raised in the first instance with the Principal and/or the Designated Safeguarding Lead (DSL). Concerns or queries about this policy can be addressed with any member of staff or the Principal.

By fostering collaboration between the school and parents, we aim to create a unified approach to online safety, ensuring that all members of the school community are actively engaged in maintaining a secure digital environment.

6. Communication and Digital Tools

6.1 Email

- **Policy Statement:** Email communication is an essential tool for staff and pupils at St. Joseph’s Catholic Primary School. All email communication must be conducted professionally, with due regard to the security and safety of personal and school information.
- **Guidelines for Staff:**
    - **School Email System:** The school email system is provided, filtered, and monitored by Link2ICT and the IT team. Staff members are issued with a school email address, which must be used for all professional communication, in line with the **Acceptable Use Policy (AUP)**.
    - **Access to Personal Email Accounts:** Staff are permitted to access their personal email accounts on school devices outside of directed teaching time. However, they must adhere to the school’s email procedure and understand that all email activity is monitored and any email sent via school equipment will be scanned by the monitoring software for security.
    - **Security and Monitoring:** All email accounts are subject to security monitoring. Staff must ensure that their messages comply with the school’s email policy. Any inappropriate or suspicious email activity should be reported immediately to the class teacher or the Online Safety coordinator.
- **Guidelines for Pupils:**
    - **School Email Addresses for Pupils:** Pupils in Key Stage 1 have access to class-based email accounts, which are monitored by the class teacher. Key Stage 2 pupils are issued with their own school email address for class-based activities.
    - **Monitoring of Pupils’ Emails:** The school email system is monitored for security purposes. Pupils must understand that their email communication is not private and will be scanned for safety. They should use their email accounts responsibly and in accordance with the guidelines set out by the school.
    - **Email Security and Reporting:** Pupils are educated on how to compose and structure emails appropriately. If any inappropriate emails are received, they must report them immediately to the class teacher or Online Safety coordinator.
- **Security Measures:**
    - **Regular Password Changes:** St. Joseph’s encourages all staff and pupils to change their passwords regularly to enhance the security of email accounts and to protect the personal and school data being communicated via email.

6.2 Published Content and Digital Media Use

- **Editorial Responsibility:** The Principal holds ultimate responsibility for content published on the school website but delegates the editorial duties to appropriate staff members.
- **Copyright:** The school retains copyright over any material published on its website. If external content is used, permission will be obtained from the copyright holder before publication, with appropriate attribution.
- **Contacting the School:** The school encourages the use of email for contacting the school via generic office email addresses and staff-specific addresses. However, the school will not publish contact details for pupils.

6.3 Digital and Video Images of Pupils

- **Parental Permission:** Parental permission is requested at the start of each school year regarding the use of photographs/videos of pupils on the school website, in local press, and for displays within the school. Written consent is required for each student.
- **Image Guidelines:**
    - o Group photos will be used where possible, with general labels/captions.
    - o Names and images will not be used together; if a pupil's name is used, their image will not be.
    - o The website will not contain home addresses, phone numbers, personal emails, or other personal information about pupils or staff.

6.4 Storage of Images

- **Centralized Storage:** Digital and video images of pupils will be taken with school equipment and stored in a central, secure area. Access is limited to teaching staff and the IT network manager.

6.5 Digital Media Policy:

- **Parental Consent:** Written permission will be obtained from parents/carers, governors, staff, and pupils before images or videos are published or distributed outside the school.
- **Privacy and Publication Guidelines:** All photographs and videos will adhere to current guidelines (such as Becta or other government standards), ensuring that individual students are not identified without explicit consent.

6.6 Video Conferencing Policy:

- **Permission and Supervision:** Pupils must obtain their teacher’s permission to participate in video conferencing. All video conferencing sessions must be appropriately supervised based on the age of the pupils, ensuring a safe and secure learning environment.

7. Monitoring, Access Control and Technology Use

This section outlines how St. Joseph’s Catholic Primary School ensures the appropriate monitoring and control of internet and network use to safeguard all users, while also addressing the safe and responsible use of mobile and emerging technologies within the school community.

7.1 Monitoring and Access Control:

To ensure the security of both the school network and its users, the following monitoring and access control procedures are in place:

- **Pupils' Use:** Pupils' use of technology is closely monitored by staff, who are always present during technology use to ensure that students are using digital resources responsibly.
- **Staff Use:** Staff internet and network usage is monitored by the Principal, Online Safety Co-ordinator, and IT Team, ensuring compliance with school policies.
- **Access Credentials:**
    - o All staff are issued with unique usernames and passwords for network access, ensuring that usage can be traced back to the individual.

    - Visitors and supply staff are issued temporary IDs, and their details are recorded in the school office to monitor and control access to the network.
    - **Key Stage 1 Pupils:** These students use class logon IDs for their network access.
    - **Key Stage 2 Pupils:** Students are given individual usernames and passwords and are educated on the importance of not sharing these credentials.

7.2 Technology Use and Security:

The school is committed to ensuring that all digital devices, both personal and school-issued, are used securely to protect the school's network and systems.

- **Acceptable Use Policies (AUP):** The school's Acceptable Use Policies apply to all equipment, whether on or off-site, including personal devices. Staff members are expected to follow these policies to maintain the security of the school's network and IT infrastructure.
- **Use of Personal Devices:** Staff members must not connect personal devices to the school network without prior approval to prevent potential security risks. Personal devices should be used responsibly in line with the school's technology policy.
- **Mobile Phones:**
    - **Staff:** Staff are reminded to use mobile phones sensibly, in line with school policy, to prevent disruptions to the learning environment.
    - **Pupils:** The school discourages pupils from bringing mobile phones to school due to concerns about bullying, harassment, and misuse. However, if a pupil must bring a phone for safety or communication reasons, a signed permission slip from the parent or guardian is required. The phone will be kept in the school office for the day and collected at the end of the school day.
    - **Confiscation:** In line with the Education and Inspections Act 2006, the Principal has the authority to confiscate mobile devices if there is a reasonable suspicion of misuse. Confiscation will be done at the Principal's discretion and according to school policy.
    - **Photos and Videos:** Pupils and staff are prohibited from taking photos or videos of other students or staff members with personal devices unless prior consent has been given. This policy aims to safeguard privacy and prevent the inappropriate use of technology.

7.3 Emerging Technologies:

As new technologies emerge, the school evaluates their educational benefits and associated risks before allowing their introduction to the school community.

- **Evaluation and Risk Assessment:** Any new or emerging technologies will be carefully assessed to ensure they align with the school's vision for safe, effective, and responsible learning. This evaluation will consider both the potential benefits and the risks to the safety of students and staff.

By ensuring strict monitoring, implementing clear guidelines for technology use, and regularly assessing emerging technologies, the school fosters a secure and responsible digital environment for both students and staff.

8. ICT Health and Safety Guidelines

Safe Working Environment: The school has created a safe ICT working environment for both pupils and teachers, adhering to health and safety guidelines.

Supervision: Pupils are supervised while using interactive whiteboards and digital projectors to ensure their safety.

9. Cyberbullying, Social Media and Online Communication Policies

9.1 Policy Review and Use of Social Networking and Online Communication:

- The school regularly reviews the use of social networking sites and online communication tools to ensure the safety and well-being of all users. Currently, access to these sites is not permitted for students during school hours.

9.2 Guidance on Safe Use of Social Media and Online Communication:

The school provides clear guidance on the safe and responsible use of social networking sites and online communication tools. This includes:

- Avoiding the publication of personal information.
- Not sharing details about the school community.
- Setting appropriate privacy settings on personal accounts.
- Reporting inappropriate content or issues promptly.

9.3 Unmoderated Chat Sites:

Unmoderated chat sites are blocked by the school's filtering systems. Students are educated about the dangers of such sites, with age-appropriate advice on avoiding them.

9.4 Cyberbullying and Social Media Policy:

Cyberbullying is a serious issue that the school addresses thoroughly. Any instances of cyberbullying, whether involving pupils or staff, will be dealt with in accordance with the school's Behaviour Policy, Anti-Bullying Policy, and Safeguarding Procedures.

10. Cyberbullying Policy

10.1 Definition:

Cyberbullying occurs online, through platforms such as social networking sites, messaging apps, or gaming sites. Like other forms of bullying, it involves the repetitive, intentional harming of an individual or group by another, where there is an imbalance of power.

10.2 Preventing and Addressing Cyberbullying:

To prevent and address cyberbullying:

- Pupils will be educated on what cyberbullying is, what to do if they experience or witness it, and how to report it.
- Class teachers will actively discuss cyberbullying with students, explaining its forms and consequences.
- As part of the curriculum, aspects of personal, social, health, and economic (PSHE) education will include discussions on cyberbullying.
- All staff, governors, and volunteers (where appropriate) will receive training on cyberbullying as part of safeguarding training.
- The school will provide information and leaflets on cyberbullying to parents/carers to help them understand the signs and how to support their children.

For any specific cyberbullying incident, the school will follow the processes set out in the Behaviour Policy. If harmful, inappropriate, or illegal material is shared among pupils, the school will act promptly to contain the incident.

- Cyberbullying involving sexual harassment, such as the sharing of indecent images or videos, will be handled in line with the school's safeguarding policy and may involve external services.

- The Designated Safeguarding Lead (DSL) will report incidents to the police if illegal material is involved and will collaborate with external agencies if necessary.

10.3 Artificial Intelligence (AI):

Generative AI tools, like chatbots (e.g., ChatGPT and Google Bard), have widespread use and can enhance learning, but they also pose risks for misuse. The school recognises that AI could be used to bully others, such as through the creation of "deepfakes" — realistic but manipulated images, audio, or video intended to deceive or harm.

- Any use of AI tools for bullying will be treated in accordance with the Behaviour Policy.
- Staff should assess the risks of new AI tools being introduced and ensure that students understand how to use such technologies safely and ethically.

10.4 Deepfakes and AI Misuse:

The misuse of AI, including the creation of deepfakes, AI-generated bullying, or using generative tools for manipulation or harassment, is a serious offence under this policy. Any incidents involving the use of AI to harm or deceive will be logged and handled in line with the school's safeguarding and behaviour policies. Staff must carry out a risk assessment for any AI tools introduced into the curriculum, ensuring that students understand the ethical implications and safe use of these technologies.

11. Acceptable Use of the Internet in School

All pupils, parents/carers, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors, when applicable, will be asked to read and agree to the school's terms on acceptable use.

- **Staff Responsibilities**: Staff are expected to model positive online behaviour and demonstrate the safe and respectful use of digital technologies. Any breach of acceptable use by staff will be dealt with in accordance with the staff code of conduct.
- **Educational Use**: The use of the school's internet is strictly for educational purposes or for fulfilling the duties of an individual's role. Personal use should be limited and must comply with the school's guidelines.
- **Monitoring and Filtering**: The school will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with acceptable use. Access to websites will be restricted through filtering systems where appropriate.

12. Responding to Incidents and Breaches

The school takes any misuse of ICT systems or the internet seriously and has clear procedures in place for responding to incidents. The action taken will be based on the nature, seriousness, and individual circumstances of the specific incident, ensuring that the response is proportionate.

12.1 Incident Response and Reporting:

• **Handling of Inappropriate Use:** Any inappropriate use of school resources will be dealt with in line with the school's policies, including the Behaviour Policy, Anti-Bullying Policy, and Safeguarding Policy.
• **Illegal Activity:** Any suspected illegal activity will be reported directly to the police. The IT Team and Link2ICT Service Desk will be informed to provide local authority support.
• **Staff Misconduct:** Any breach of policy by staff will be investigated by the Principal. Action may be taken under the Birmingham City Council/MAC Disciplinary Policy, with serious breaches potentially leading to dismissal.
• **Pupil Misconduct:** Serious breaches by pupils will be investigated thoroughly, and appropriate records will be kept. For serious breaches, the incident may lead to exclusion. Disciplinary action will depend on the specific circumstances of the misuse, following the procedures outlined in the Behaviour Policy and Acceptable Use Agreement.
• **Staff Misuse:** If a staff member misuses the school's ICT systems or internet, or misuses a personal device in a way that constitutes misconduct, the matter will be addressed in line with the staff code of conduct. The

response will be proportionate and based on the seriousness of the incident.
• **Illegal or Serious Incidents:** In cases of illegal activity, inappropriate content, or other serious incidents, the school will consider whether the matter should be reported to the police.

13. Training

All new staff members will receive comprehensive training as part of their induction on:

- Safe internet use
- Online safeguarding risks, including cyber-bullying and online radicalisation
- Their roles and responsibilities regarding the school's filtering and monitoring systems

All staff will receive refresher training **at least annually** as part of safeguarding training. This will include updates on:

- New and emerging online threats, such as AI-driven exploitation, digital grooming, and deepfake abuse
- Peer-on-peer abuse in online environments
- Platform-based risks as identified in the **Online Safety Act 2023/24**

Regular safeguarding updates will also be provided throughout the year via emails, e-bulletins, and staff meetings to ensure continued awareness and responsiveness.

Through this training, staff will be made aware that:

- Technology is a significant factor in many safeguarding and wellbeing issues
- Children may be at risk of online abuse, including from peers
- Online peer abuse can include:
  - Abusive, harassing, or misogynistic messaging
  - Non-consensual sharing of indecent images or videos (particularly in group chats)
  - Sharing of explicit content without consent
- Physical abuse, sexual violence, and initiation/hazing incidents can also involve digital elements

Training will also help staff to:

- Recognise signs and symptoms of **online abuse**, including AI-generated threats
- Ensure pupils can identify risks, assess dangers, and seek help when needed
- Support pupils in making **safe, healthy, and informed decisions online**

14. Additional Responsibilities:

- The **DSL** will undertake child protection and online safety training at least every **2 years** and update their knowledge **annually or as necessary**.
- **Governors** will receive training on:
  - Online safeguarding, including AI and digital risks
  - Their responsibilities under the **DfE's Filtering and Monitoring Standards (2024)**
  - Platform accountability requirements under the **Online Safety Act**
- **Volunteers** will receive appropriate safeguarding and online safety training relevant to their role.

Further details about our safeguarding training approach are outlined in the Child Protection and Safeguarding Policy.

15. Related Documents and Links with Other Policies

This Online Safety Policy is part of a broader safeguarding framework, and it should be read in conjunction with the following key school policies, which support and inform the policy framework. These documents ensure that online safety is embedded across all aspects of school life and are integral to safeguarding, behaviour, and data protection.

15.1 Related Documents:

- Acceptable Use Policy (AUP) for Adults and Young People – Internet and Associated Communications Technologies
- Computing Policy
- Data Protection Policy
- Behaviour Policy
- Anti-bullying Policy
- Whistleblowing Policy
- Safeguarding Policy

15.2 Links with Other Policies:

This Online Safety Policy should also be read alongside the following documents that form part of the school's safeguarding framework:

- **Child Protection and Safeguarding Policy:** Outlines the school's responsibilities and procedures for safeguarding children from all forms of abuse, including those occurring online. It provides guidance on identifying, reporting, and managing safeguarding concerns that may involve online activity.
- **Behaviour Policy:** Addresses the standards of behaviour expected from pupils, including rules related to online conduct. It provides specific provisions for dealing with cyberbullying and inappropriate online behaviour, along with applicable sanctions.
- **Staff Code of Conduct:** Sets expectations for staff behaviour, including the responsible use of ICT and online resources, and outlines actions that may constitute misconduct in relation to digital technology.
- **Anti-Bullying Policy:** Complements the Online Safety Policy by detailing how bullying, including cyberbullying, will be addressed in school. It outlines procedures for prevention, intervention, and resolution of bullying issues.
- **Data Protection Policy:** Provides guidelines on the handling, storage, and sharing of personal data in accordance with the Data Protection Act 2018 (GDPR). This policy is particularly relevant for online safety, as it governs the protection of personal data when interacting online or using school resources.
- **Curriculum Policy:** Refers to the integration of online safety within the broader school curriculum, particularly in computing, PSHE (Personal, Social, Health, and Economic) education, and citizenship lessons, ensuring pupils are taught how to use technology safely and responsibly.
- **Remote Learning Policy:** Outlines how online safety is maintained during remote or blended learning sessions, including guidance on the use of school-approved digital platforms and safeguarding students in a virtual environment.

This policy should be read alongside the **Child Protection Policy**, which offers further steps for protecting children from online exploitation, peer-on-peer abuse, and the risks associated with emerging digital technologies.

All our policies can be found on our school website or via this link:
https://www.stjosutton.net/web/policies_and_forms/585421

Appendix 1: EYFS And KS1 Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

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 select 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 schoolwork only
- 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 agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Appendix 2: KS2 Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

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 usernames 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've 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
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- 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, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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

Signed (pupil):	**Date:**

Appendix 3: Staff Acceptable Use Policy (AUP)

St Joseph's Primary School – Staff Agreement for ICT, Online Safety and Digital Technology Use

This Acceptable Use Policy outlines the expectations and responsibilities for all staff, including supply teachers, support staff, volunteers, contractors, and governors, in relation to the safe, legal, and professional use of technology in our school.

By signing this policy, you agree to use the school's digital resources and systems in a responsible, ethical, and secure manner to protect pupils, yourself, and the wider school community.

---

1. Safe and Responsible Technology Use

- I will use all school ICT systems, software, email, and internet access for professional, educational, and school-authorised purposes only.
- I will ensure all activity under my login credentials is appropriate and secure, and I will not share my login details with others.

---

2. Data Protection and Privacy

- I will access, use, and store personal or sensitive data in accordance with the Data Protection Act 2018 (UK GDPR).
- I will only use approved cloud storage and devices to handle school data, and never transfer data to personal devices or unsecure platforms.
- I will lock screens when away from my device and store any printed sensitive data securely.

---

3. Internet and Email Usage

- I will communicate professionally in all digital interactions with pupils, parents, colleagues, and external agencies.
- I will not use personal email, social media, or messaging apps to communicate with pupils or parents.
- I understand that my digital activity on school systems is monitored and may be reviewed.

---

4. Use of AI and Emerging Technologies

- I will only use AI tools and platforms that have been approved by school leadership or the ICT manager.
- I understand that I must not generate or share AI-created content that may be inaccurate, misleading, inappropriate, or harmful.
- I will report any suspected misuse of AI by pupils, including use of deepfakes, impersonation, or AI-assisted bullying, to the DSL.

---

5. Filtering, Monitoring and Digital Safeguarding

- I am aware that the school's filtering and monitoring systems are in place to protect children and staff and that my activity may be logged.
- I will immediately report any failures or breaches in filtering/monitoring to the Designated Safeguarding Lead (DSL) or ICT Manager.
- I will challenge or report any online material or activity that is illegal, unsafe, discriminatory, or harmful.

---

6. Mobile Devices and BYOD (Bring Your Own Device)

- I will only use personal devices (e.g. phones or laptops) in line with the school's mobile device policy.
- I will never use my personal device to photograph, record or share images of pupils unless explicitly authorised.
- If I connect a personal device to the school network, I understand it must meet the school's cybersecurity and safeguarding requirements.

---

7. Modelling Positive Online Behaviour

- I will model respectful, responsible, and safe behaviour when using technology with pupils or colleagues.
- I will educate pupils about safe digital habits when opportunities arise, particularly regarding privacy, AI, and social media safety.

---

8. Training and Compliance

- I will attend all mandatory online safety training and safeguarding updates, including emerging risks such as:
    - AI-generated exploitation or manipulation
    - Peer-on-peer abuse via digital platforms
    - Deepfakes or impersonation threats
- I will comply with all school safeguarding and online safety policies and report concerns using school safeguarding procedures.

Breaches of Policy

I understand that breaches of this policy may result in disciplinary action, in line with the **Staff Code of Conduct** and **Safeguarding Policy**, and where appropriate, referral to external safeguarding authorities.

Staff Declaration

I have read, understood, and agree to comply with the St Joseph's Primary School **Staff Acceptable Use Policy** for 2025–2026. I will follow all guidance in this document and the wider safeguarding framework to keep pupils and myself safe online.

Full Name ________________________________

Position/Role ________________________________

Signature ________________________________

Date ________________________________

Appendix 4: Online Safety Training Needs – Self-Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	