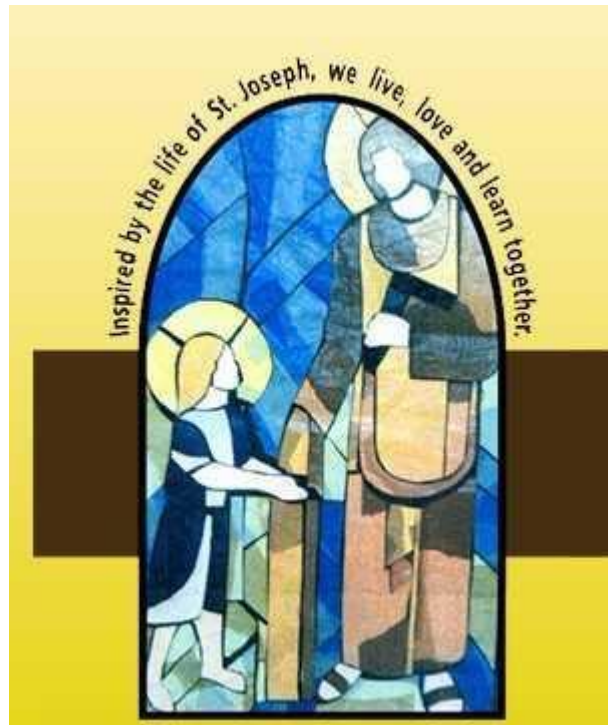


# **Online Safety Policy**

## **St Joseph's Catholic Primary**

*We follow in St. Joseph's footsteps, building a community of love, trust, respect and learning.*



**Reviewed by Samantha Golding September 2025**

**Approved by Governors**

**Date  
November 2025**

*To be reviewed annually*

## **Online Safety Policy**

***We follow in St. Joseph's footsteps, building a community of love, trust, respect and learning***

Whilst care has been taken to consider all aspects of online safety, there may be times when members of staff, schools and services need to make independent judgments on individual situations not covered in this document. It is expected that in these circumstances that all staff will advise their senior colleagues of such action taken or proposed and the school will see further advice.

This document applies to all members of staff employed directly by St Joseph's Catholic Primary School. All members of staff are expected to adhere to this code of practice to ensure the safety of the pupils in their care and in doing so fully abide by the guidance contained herein. Any member of staff found to be in breach of these guidelines may be subject to disciplinary action.

For the purpose of the document, 'children', 'pupils' and 'young people' will refer to all children and young people who members of staff have contact with as part of their professional capacity and to which all staff have a professional duty of care.

### **Aim**

The aim of this policy is to ensure that the whole school community, adults and pupils, are aware of the safety issues associated with information systems and electronic communications. Its purpose is to allow all members of our community to enjoy the many benefits of electronic communication whilst understanding the dangers and taking appropriate precautions to keep themselves safe.

Online safety encompasses not only Internet technologies but also electronic communications such as mobile phones, social networking, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day – if it is used safely.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children. The popularity of social media can also bring with it unwanted issues such as cyber-bullying and children need to be equipped to know how to deal with

any issues that arise. Pupils must also learn that publishing personal information could compromise their security and that of others.

Online safety depends on effective practice at a number of levels:

- Responsible IT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of the Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including an effective filtering/fire wall.

The Online Safety Policy relates to other policies including those for Code of Conduct and for child protection and anti-bullying.

### **Policy and Leadership**

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

#### **Headteacher and senior leaders**

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher is responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

#### **Governors**

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. . A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant governors group/meeting
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- membership of the school Online Safety Group

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

### **Designated Safeguarding Lead (DSL)**

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

### **Curriculum Lead**

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme. This will be provided through a discrete programme (ProjectEVOLVE) and through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

## **Teaching and Learning**

The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The use of the Internet will enhance learning.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught which Internet use is acceptable and what is not and given clear objectives for Internet use including keeping themselves safe and legal online.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate Internet content and use and develop their critical thinking skills.
- Pupils will be taught how to recognise techniques used for persuasion online (eg fake news and grooming).
- Pupils will be taught how to seek support if they are concerned by something they view online.
- Pupils will be taught how to effectively navigate the internet and manage information.
- Pupils will be taught about the effects of online use on general well-being (eg about self-image and identity, managing screen use).

If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Head of School who will report it to the broadband provider. The School should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read.

### **IT Provider**

It is the responsibility of the school to ensure that the IT provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack

- the school meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

### **Social Contact with Pupils**

Staff must not establish social contact with pupils, children or young people for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a pupil, child or young person seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise his or her professional judgment and inform their senior colleagues. All contact with pupils, children or young people should be through appropriate channels at all times.

Staff should not give, nor be required to give their personal details such as home or mobile phone number, instant messenger identities or personal e-mail address to pupils, children or young people. Staff should not use any of the above means to contact pupils, children or young people.

Members of staff should:

- Always seek approval from senior management for any planned social contact with pupils, children or young people.
- Advise senior management of any regular social contact they have with a pupil child or young person which may give rise to concern.
- Report and record any situation which they feel might compromise the reputation of the organisation or their own professional standing.

### **Internet Use**

Members of staff must follow and adhere to the policy and must not share logins or passwords with other members of staff, pupils, children or young people, friends, family or members of the public.

Under no circumstance should members of staff in the workplace access inappropriate images using either personal or work-based equipment.

### **Mobile technologies**

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation.

School owned/provided devices:

- all school devices are managed through the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- any designated mobile-free zone is clearly signposted
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectations are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- where personal devices are brought to school, but their use is not permitted,

- appropriate, safe and secure storage should be made available
- use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes

### **Information System Security**

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly
- The school uses the London Grid for Learning (LGfL) with its firewall and filters.

### **E-Mail**

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils must only email people teachers/school has approved
- Emails sent must always be polite and friendly.
- Email sent to an external organisation will be written carefully and authorised before sending, in the same way as a letter written on school headed paper. Pupils must not open emails from people they don't know.
- The forwarding of chain letters is not permitted.

### **Filtering and Monitoring**

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility. The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a

change in working practice, e.g. remote access or new technology is introduced.

### Filtering

- The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

### Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention (see Appendix A).
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring leads

## AI

AI must be used in accordance with the AI Policy.

Before using any AI system, staff must:

- consult the AI register
- confirm that the AI tool is listed and approved for the intended use
- familiarise themselves with the permitted uses and any restrictions recorded in the AI Register
- report any misuse, unauthorised access or data protection concerns promptly

In terms of expected professional standards and behaviours, staff are expected to:

- understand that AI is a support tool designed to enhance teaching and delivery but is never a substitute for professional judgement
- understand that the quality and content of any final material(s) remains their responsibility
- remain responsible and accountable for the accuracy, appropriateness and quality of any AI generated material they use or adapt, including in contexts such as:
  - o creating or adapting educational resources
  - o planning lessons or curriculum content
  - o drafting tailored feedback or revision materials
  - o supporting administrative tasks such as report writing or meeting preparation

Staff must not use AI systems:

- to make decisions that carry significant consequences for pupils or staff (e.g. safeguarding, behaviour, performance, SEND)
- to assess subjective work without applying their own professional judgment
- to impersonate others or present AI-generated work as wholly human-authored
- for any purpose that is unlawful, misleading or outside the scope of approved use

Staff are expected to uphold all relevant legal and regulatory standards when using AI, including:

- data protection and UK GDPR
- copyright and intellectual property rights
- equality legislation
- duties under Keeping Children Safe in Education

## THINK BEFORE YOU CLICK!!

### **Published content and the school web site**

The contact details on the web site should be the school address, email and telephone number. Staff or pupils personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The school web site will have links to online safety sites for parents.

### **Publishing pupils' images and work**

Written permission from parents or carers to publish work/photos will be obtained when the child starts school. This permission slip will be kept on the child's school file. Pupils' work is chosen carefully before publishing e.g. to check it does not contain personal information.

### **Photos and videos**

Work-based activities involve the use of recording images and/or videos, and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. School devices must be used. Written permission should be gained before any photography or videography takes place.

Photograph or video images where possible must be created using equipment provided by the workplace. **Use of personal mobile phones are not to be used when photographing children.** Photograph or video images must be created using equipment provided by the workplace.

### **Social Media**

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to personal social media sites during school hours
- Monitoring of public social media
- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- the school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

### **Managing emerging technologies**

Technologies within this policy include: websites, email, instant messaging, chat rooms, social media, mobile phones, blogs, podcasts, downloads and virtual learning platforms. New technologies are always emerging and this is not an exhaustive list.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils should not use mobile phones at school or on school trips. The sending of abusive or inappropriate text messages is wrong. Any phones brought to school (eg if a pupil walks home alone in the evening) must be handed in and stored securely in the phone safe located in the school office.
- If pupils/adults use mobile phones or other technologies inappropriately then sanctions will be implemented. A phone safe is provided for staff in the staff room.

### **Authorising Internet Access**

- All staff and pupils are granted Internet access, although access could be denied in the event of inappropriate use.
- In the Early Years Foundation Stage pupils are only able to access the sites and software specifically designed for their needs under staff supervision.
- At Key Stage 1 & 2, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials (safe searches).
- Assessing risks
- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of 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 Headteacher will ensure that the Online Safety Policy is implemented and practice compliance with the policy monitored.

## **Peer on Peer Abuse (Child on Child)**

All staff should be aware that children can abuse other children (often referred to as peer on peer abuse). Peer on peer abuse can happen online and it is important that all staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports. It is important for all staff to challenge inappropriate behaviour between peers that are actually abusive in nature. Peer on peer abuse involving technology is most likely to include, but may not be limited to:

cyberbullying, sexual harassment, consensual and non-consensual sharing of inappropriate images and/or videos, upskirting, initiation/hazing type violence and rituals.

## **Handling online safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- All internet misuse must be logged on the Online Safety Incident Log (Appendix A)
- Any complaint about staff misuse must be referred to the Head of School.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Sanctions within the school discipline policy include:
  - interview/counselling by class teacher or head teacher
  - informing parents or carers
  - removal of Internet or computer access for a period

## **Community use of the Internet**

- The school will be sensitive to Internet related issues experienced by pupils out of school e.g. social networking sites, and offer appropriate advice.

## **Introducing the Online Safety Policy to pupils**

- Internet Safety posters will be posted around the school by every computer as well as the SMART rules.
- Pupils will be informed that Internet use will be monitored and can be traced back to the user through their username.
- Staff can refer to the 'Education for a Connected World Framework' for age-specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

## **Online Safety Education Programme**

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. SMILE
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

### **Vulnerable Pupils**

We acknowledge that certain pupils are more vulnerable to the dangers of keeping safe online; this could include pupils with SEND. During online safety lessons specific differentiation is made by teachers to support the needs of our most vulnerable pupils. We acknowledge that at any given time any pupil can be vulnerable online (age, developmental stage and personal circumstance). Teachers can access the STAR SEN Toolkit to support planning and differentiation for vulnerable pupils.

### **Staff and the Online Safety Policy**

All staff will be given the School Online Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff will be able to access appropriate training annually to develop their own understanding of online safety and emerging trends and needs. This may be online training, external speakers, courses or in-house led CPD.

### **Enlisting parents' support**

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

### **Data Protection**

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy

- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected. (Be sure to select devices that can be protected in this way)
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).

- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

The Online Safety Policy will be reviewed annually.

This policy has been reviewed using the following guidance:

- Education for a Connected World – 2020 edition
- Keeping Children Safe in Education 2025

St. Joseph’s Catholic Primary School

Online safety Incident Log

| Date | Description of Incident | Reported to | Reporting Procedure followed | Action Taken | Policy and Practice reviewed | Outcome |
|------|-------------------------|-------------|------------------------------|--------------|------------------------------|---------|
|      |                         |             |                              |              |                              |         |
|      |                         |             |                              |              |                              |         |
|      |                         |             |                              |              |                              |         |
|      |                         |             |                              |              |                              |         |