St Joseph's Catholic Primary School

Online Safety Policy

Mission Statement

Following in the footsteps of Jesus; we live, love and learn.

Inclusion Statement

In this school, we are educating our children to:

- know who they are - a special and unique gift from God
- know why they are here - we all have a purpose and responsibility to look after God's world
- work hard and aim high for their future - find and use their God given talents to become everything that God intends them to be

We are a Catholic community, in a modern society, where everyone is equal. As a Catholic School, we strive to reflect the teachings of Christ and live out the Gospel Values in everything that we do. The most loving and merciful Jesus Christ is our role model, and He welcomed everyone. All children are welcome in our school; they and their families become part of our St. Joseph's family. We will love and nurture them, and do our best to help them to become everything that God intends them to be.

At St Joseph's Catholic Primary School our values reflect our commitment to a school where there are high expectations of everyone. Children are provided with high quality learning opportunities so that each child attains and achieves all that they are able to. Everyone in our school is important and included. We promote an ethos of care and trust where every member of our school community feels that they truly belong and are valued. We work hard to ensure there are no invisible children here, recognising everyone's uniqueness and success. We recognise learning in all its forms and are committed to nurturing lifelong learners. We are a safe school, committed to improving children's confidence and self-esteem. We know that safe and happy children achieve.

Adopted by Governors	*(signed on hard copy)*
Date	**10.10.2025**
Review Date	**10.10.2026**

RATIONALE

The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide our learners with Internet access as part of their learning experience.
St Joseph's Catholic Primary School believes that this access must ensure the safeguarding of all learners.

Online Coordinator:	Mrs A Douglas, Mr K Broomhead
ICT Coordinator:	Mr K Broomhead
Child Protection Officer:	Mrs A Douglas

1.1 Internet use to enhance and extend learning

- St. Joseph's Internet access is designed expressly for pupil use and includes filtering appropriate to the age and needs of pupils.
- Clear boundaries will be set for the appropriate use of the internet and digital communications and discussed with staff, pupils and parents.
- Pupils will be educated in the effective use of the Internet in research, how to critically evaluate the materials they read and shown how to validate information before accepting its accuracy through our ICT curriculum.
- We will ensure that the use of Internet derived materials will comply with copyright law.
- SEN children will be taught alongside their peers; materials will be used that match the needs of these learners.

1.2 Managing Internet Access

- 1.2.1. Information system security
  - St Joseph's ICT system security will be reviewed regularly by blocking any inappropriate content using 'FortiGuard Intrusion Prevention'. Network Connect are contracted by school to manage 'FortiGuard Intrusion Prevention, on school's behalf. If changes need to be made i.e. a webpage is blocked which shouldn't be, a request will be sent to unblock it.
  - Virus protection will be installed and updated regularly by Network Connect.
- 1.2.2 E-mail and messaging
  - Pupils must immediately tell a teacher if they receive an offensive e-mail or message.
  - In any e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
  - Attachments should be treated as suspicious and not opened unless the author is known
  - The forwarding of chain e-mails is not allowed
- 1.2.3 Published content on the school website*

*(*school website includes .uk)*

  - Any online contact details used for staff, should be their 'sch.uk' e-mail address or the school office e-mail. Any pupil contact details must be given as the school office e-mail.
  - The members of staff given overall responsibility for the website will take overall editorial responsibility and ensure that published content is accurate and appropriate.
- 1.2.4 Publishing pupils' images and work
  - Written permission from parents will be obtained before photographs of students are published on the school website this can be found in the school admissions forms.
  - Work can only be published with the permission of the pupil.
- 1.2.5 Social Networking and personal publishing
  - St Joseph's will control access to social networking sites, and consider how to educate pupils in their safe use.
  - School issues should not be discussed on external social networking sites by staff, parents or children.
  - Newsgroups will be blocked unless a specific use is approved by the ICT coordinator.
  - Pupils are advised never to give out personal details of any kind which may identify them, their family, friends or their location.

- Pupils are encouraged to set strong passwords, to deny access to unknown individuals and block unwanted communication. Only known friends should be invited and access denied to others.
- SEN children are subjected to these same high standards; however, time is given to ensure understanding and appropriate language and materials are used.

- 1.2.6 Managing Filtering
  - The school will work in partnership with Network Connect to ensure that the systems in place to protect our pupils are reviewed and improved.
  - If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Co-ordinator.
  - The ICT coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- 1.2.7 Managing Videoconferencing
  - IP video conferencing rights and privileges will be monitored and controlled by the ICT coordinator.
  - Pupils must seek permission from the supervising teacher before answering or making a video conference call.
  - Video conferencing must appropriately be supervised for the pupils' ages.

Please see our Remote Learning Policy for further information related to online interaction using video conferencing software in lockdown and isolation periods during COVID-19

- 1.2.8 Managing Emerging Technologies
  - Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.
  - Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
  - Therefore, mobile phones should not be used at any time during the school day.
  - The use by students of mobile phone cameras is not allowed. If a photograph is needed, school iPads must be used.
  - Staff should not contact students directly with their own mobile phones unless in exceptional circumstances and a member of the SLT has been informed. Staff should be vigilant to avoid the receipt of items via Bluetooth whilst in school.
- 1.2.9 Protecting Personal Data
  - Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018.

1.3 Policy Decisions

- 1.3.1 Introducing the Online Safety Policy
  - All staff must read and sign the 'Staff Code of Conduct for ICT' to allow use of the school ICT resources.
  - A list of all current staff and pupils granted access to school ICT systems will be maintained.
  - Pupils must also apply for Internet access individually by agreeing to comply with the Responsible Use Statement on view in all rooms with ICT resources. This will be explained more fully for our SEN children to ensure compliance and understanding of what is being asked.
  - Parents/Carers are also asked to sign and return a consent form.

- 1.3.2 Assessing Risks
  - The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school, nor Network Connect can accept liability for any material accessed, or any consequences of Internet Access.

- The school will annually audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the policy is appropriate and effective.

- 1.3.3 Handling Complaints
  - Complaints of Internet misuse will be dealt with primarily by the class teacher, then if further support is needed, escalated to the ICT and Online Safety Coordinator.
  - Any complaints about staff misuse must be referred to the ICT and Online Safety Coordinator and the Headteacher.
  - Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.
  - Discussions will be held with the Police or Community Support Officers to establish procedures for handling potentially illegal issues.

1.4 Communicating Online safety

- 1.4.1 Introducing the Online Safety Policy to pupils
  - Online Safety rules will be posted in all rooms where computers/iPads are accessed.
  - Pupils will be informed that all network and internet use will be closely monitored.
  - Training in Online Safety will be developed based on the materials suggested by, Lancashire, and delivered to pupils via assemblies and through lessons in class relevant to their age, need and relevant issues arising in class.
- 1.4.2 Staff and the Online Safety Policy
  - All staff will be given the policy and its importance will be explained.
  - Staff will be informed that Network and Internet traffic can be monitored and traced to the individual user.
  - Staff managing filtering systems and monitoring ICT use will be overseen by the ICT Coordinator and will follow the clear procedures set out for reporting issues. (see appendix)
- 1.3.3 Enlisting Parents' and Carers' Support
  - Parents' and Carer's attention will be drawn to the school Online Safety Policy on the school website and via parent information evenings.

Signed …….

Head teacher

Date ……

Signed ……

Chair of Governors

Date ……

Appendix 1

Staff Procedures for Breeches of the Policy

1) If a teacher finds unacceptable material on a pupil's account or screen:
    a. **DO NOT PRINT OFF ANY PORNOGRAPHIC MATERIAL**
    b. Alert the Online Safety Co-ordinator
2) If a pupil reports any cyber bullying issue (malicious text, email, messages) to a member of staff:
    a. Record the incident on CPOMs *(Child Protection Online Monitoring System)* Who, What, When – Actions taken
    b. Refer the incident to the relevant Online Safety Coordinator
    c. The Online Safety Coordinator should report the incident to the Headteacher

Appendix 2

Online Safety Policy Summary for Parents
Online Safety Coordinator – Mr K Broomhead

What is Online Safety?

Online Safety encompasses the use of new technologies, Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguarding and awareness for users to enable them to control their online experience.

End to End Online Safety

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

- Responsible I.C.T. use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Network Connect including the effective management of filtering.

Writing and reviewing the Online Safety Policy

- The Online Safety Policy is part of the School Development Plan and relates to other policies including those for I.C.T., Anti-Bullying and for Child Protection.
- Our Online Safety Policy has been written by the school and from government guidance. It has been agreed by senior management and approved by the Governors.
- The Online Safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet use is important
- 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.

Internet use 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 what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated 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.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School I.C.T. systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Network Connect.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive any offensive e-mails.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information will not be published.

Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils or pupils' work are published on the school web site. This is done through the admissions process to school.

Social Networking and Personal Publishing

- The school will block/filter access to social networking sites apart from class Twitter accounts where the teacher has sole responsibility of the content published.
- School issues should never be discussed on social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

- The school will work with the LA, DFES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.
- The I.C.T. Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are not permitted at any time in school. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff pupils and parents must read and adhere to the 'Acceptable I.C.T. Use Agreement' before using any school I.C.T. resource.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.

Assessing risks

- 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. Neither the school nor Network Connect can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit I.C.T. provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by the Online Safety Coordinator.
- Any complaint about staff misuse must be referred to the Online Safety Coordinator and the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- External organisations using the school's I.C.T. facilities must adhere to the Online Safety Policy.

Communicating the Online Safety Policy to children

Introducing the Online Safety Policy to pupils

- Children will sign the Online Safety agreement before being allowed to use the network and internet.
- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that all Network and Internet use will be closely monitored.

Reviewed by Staff and Governors October 2025
This Policy will be reviewed every year

St Joseph's Primary School Staff Code of Conduct for ICT

To ensure that all members of staff are fully aware of their professional responsibilities when using information systems and when communication with pupils, you are asked to sign this code of conduct. Members of staff should consult the school's Online Safety Policy for further information and clarification

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the ICT Coordinator or Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any instances of concern regarding children's safety to the Online Safety Coordinator and the Designated Safeguarding Lead.
- I will ensure that electronic communications with pupils including e-mail are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I am aware that images and text posted on public sites may be viewed by pupils and their parents. I will strive to ensure that my professional status will not be affected by anything I post in the public domain.
- I will not discuss school issues on any social networking sites.
- I will promote Online Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I understand that breeches of this Code of Conduct may result in disciplinary action being taken.

St. Josephs Primary School may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I confirm that I have read, I understand and accept the Staff Code of Conduct for ICT

Signed …… Date …….

Name……