Online Safety Policy

Name of School	**St Edward's Catholic Primary School**
Policy review date	**September 2025**
Date of next review	**September 2026**
Who reviewed this policy?	**Ms S Naz & Mrs N Middleton**

Introduction
Online safety (formerly E-Safety) involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and computing environment for St Edward's school.

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.
While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

• Access to illegal, harmful or inappropriate images or other content
• Unauthorised access to / loss of / sharing of personal information
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing / distribution of personal images without an individual's consent or knowledge
• Inappropriate communication / contact with others, including strangers
• Cyber-bullying
• Access to unsuitable video / internet games
• An inability to evaluate the quality, accuracy and relevance of information on the internet
• Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Online Safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and computing environment for St Edward's R.C School.

Teaching and Learning

The Internet is an essential element for education, business and social interaction.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Online Safety is taught in a detailed unit in every year group as a part of the Purplemash scheme of work.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and

parents are provided with information relating to Online Safety and agree to its use:

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any

  school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet

  access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

Social Networking

Social networking Internet sites (such as Snapchat, Facebook & TikTok) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.

- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites.

This policy applies to all members of St Edward's community (including staff, students / pupils, volunteers, governors, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of St Edward's

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

St Edward's will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Role	Key Responsibilities
Online Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that Online Safety education is embedded across the curriculum • liaises with school ICT technical staff • To

	communicate regularly with SLT and the designated Online Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident • To ensure that an Online Safety incident log is kept up to date • Facilitates training and advice for all staff • Liaises with the Local Authority and relevant agencies • Is regularly updated in Online Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: •sharing of personal data •access to illegal / inappropriate materials •inappropriate on-line contact with adults / strangers •potential or actual incidents of grooming

	•cyber-bullying and use of social media
Governors / Online Safety governor	• To ensure that the school follows all current Online Safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor • To support the school in encouraging parents and the wider community to become engaged in Online Safety activities • The role of the Online Safety Governor will include:

	•regular review with the Online Safety Co-ordinator / Officer (including Online Safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the Online Safety element of the Computing curriculum • To liaise with the Online Safety coordinator regularly
Network Manager / technician	• To report any Online Safety related issues that arises, to the safeguarding lead and class teacher and subject leader. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the

	security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices •the school's policy on web filtering is applied and updated on a regular basis •LGfL is informed of issues relating to the filtering applied by the Grid •To keep up to date with the school's Online Safety policy and technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant [Text Box]•To ensure the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator / Officer /Headteacher for investigation /

	action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager	To ensure that all data held on pupils on the school office machines have appropriate access controls in place
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts •
Teacher	• To embed Online Safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant) To ensure that pupils

	are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's Online Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the Online Safety coordinator • To maintain an awareness of current Online Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology

	• To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. •
Parents/carers	• to support the school in promoting Online Safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website / office 365+ purplemash / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology

External groups	Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Communication:
How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom/ classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:
The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include: interview/counselling by learning mentor / Online Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system
- referral to LA / Police.
- Our Safeguarding Lead acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The Online Safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an Online Safety coordinator who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online Safety policy has been written by the school Online Safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school Safeguarding policy will be discussed in detail with all members of teaching staff.

Mobile Phones

Mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the classroom teacher where they are kept in a lock box until the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phones to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers within the Foundation Stage place their phones in a locked cabinet in Nursery and Reception for the duration of hours worked by each member of staff. The remainder of staff ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom during breaks.
- Parents cannot use mobile phones on school trips to take pictures of the children.

Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff for educational use.

- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff.
- The Headteacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

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 at St Edward's Primary School Online Safety Policy. New ways of working (ie Zoom) will be trialled by staff before being rolled out to pupils and parents.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.
- Parents may upload pictures of their own child only onto social networking sites. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR requirements. The school has moved its online storage of children and staff's work to Office 365/Google Classroom and Purplemash, both of which are fully GDPR compliant.

Blended Learning

Due to situations caused by Corona Virus we have now prepared to help children access learning from home using Microsoft Teams. This has been deemed a secure way for children to interact with their pupils. All pupils have been allocated an individual secure username.

Assessing Risks

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

Communication of Policy
Pupils:

- The school participates in 'Safer internet day' by looking at how to stay safe online and various activities are planned throughout the day. Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites such as Facebook and Twitter, and on apps such as Whatsapp. This will be strongly reinforced across all year groups during computing lessons and all year groups look at different areas of safety through the digital literacy lessons.
- The school follow the Purplemash scheme of work for Online Safety.

Staff:

- 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.

Parents:

- Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the school Website.