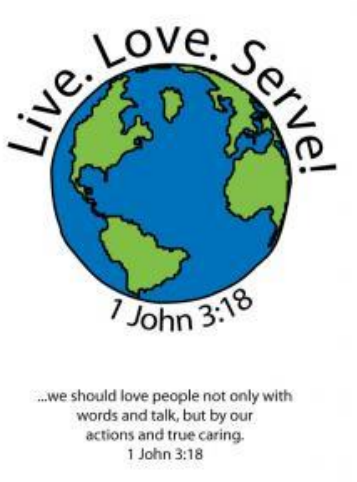
St Edward's Primary School a Catholic Voluntary Academy

Online Safety and Digital Resilience Policy

Reviewed September 2020
Review Date September 2021

Our Mission Statement



Our Vision Statement

We are guided by our Mission Statement and
we aim to:

- develop and care for the **whole child** through our teaching and sharing of the Catholic faith.
- show our love of God in the way we care and value each other and ourselves.
- aspire and equip children with those skills necessary to become contributing members of society and responsible adults.
- recognise and encourage all pupils' individual gifts and talents.
- provide an excellent quality of education striving to achieve the very highest standards for all pupils and, at the same time, develop lively critical minds.
- develop each pupil's appreciation of education as a lifelong and enjoyable process.
- work in partnership with the Parish and families, local schools and community groups recognising that only by working together can the school make its contribution towards the development of committed Christians and active members of the Church.

St Edward's Primary School
Online Safety and Digital Resilience Policy
Autumn 2020

Today, people are growing up in an increasingly digital world. Digital technologies are present in most areas of life. People socialise, explore, create and work in digital environments. Organisations, groups and communities are increasingly connected as technology becomes more pervasive. People will encounter risks during these online experiences and it is neither possible nor desirable to shield them entirely from risk. Learning how to recognise and manage risk, learn from difcult experiences, recover and stay well, is a vital part of individual development and agency. (Digital Resilience Framework, UKCIS 2019)

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for computing, bullying, PSHE and child protection.

Why the Internet and digital communications are important

The rapid developments in electronic communications are having many effects on society. The Internet is an essential element in education, business and social interaction. The school has a duty to provide pupils 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. Pupils use the Internet widely outside school and need to learn and consolidate how and to evaluate Internet information and to take care of their own safety and security.

Intent

St. Edward's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We want to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. They will be supported and encouraged to develop as responsible 21st century citizens.

Implementation

The school's Internet access is designed to enhance and extend education. The school Internet access is designed specifically for pupil use and will include filtering appropriate to all users. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use through online safety lessons. Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils are shown how to publish and present information to a wider audience. Pupils are taught how educational and cultural exchanges between pupils worldwide are effective. The school will ensure

that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils are also taught the importance of cross-checking information before accepting its accuracy as well as how to report unpleasant or inappropriate Internet content i.e. primarily by telling an adult immediately or by using the CEOP Report Abuse icon.

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time with the release of the latest devices, platforms, apps, trends and related threats. It is therefore important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. In St. Edward's this is built into existing lessons across the curriculum, covered within specific online safety lessons as well as through PSHE and Citizenship lessons that are age appropriate with a focus on progression.

Underpinning knowledge and behaviors

For pupils, underpinning knowledge and behaviours include how to evaluate what they see online to enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

In St. Edward's, lessons focus on helping pupils consider questions including

- is this website/URL/email fake? How can I tell?
- what does this cookie do and what information am I sharing?
- is this person who they say they are?
- why does someone want me to see this?
- why does someone want me to send this?
- why would someone want me to believe this?
- why does this person want my personal information?
- what's behind this post?
- is this too good to be true?
- is this fact or opinion?

Techniques for persuasion

We also help pupils to recognise techniques used for persuasion to enable them to identify the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

St Edward's help pupils to recognise

- online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation)
- techniques that companies use to persuade people to buy something
- ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- criminal activities such as grooming

Acceptable and Unacceptable online behaviour

We teach pupils to understand what acceptable and unacceptable online behaviour look like and that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Pupils are taught to recognise unacceptable behaviour in others. Pupil's learn this by

- looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do
- looking at how online emotions can be intensified resulting in mob mentality
- teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online
- considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

Identifying risks

We enable pupils to identify possible online risks and make informed decisions about how to act. This is not be about providing a list of what not to do online. This focuses on ways to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action. Pupil's identify and manage risk by

- discussing the ways in which someone may put themselves at risk online
- discussing risks posed by another person's online behavior
- discussing when risk taking can be positive and negative
- discussing "online reputation" and the positive and negative aspects of an online digital footprint, including longer-term considerations, such as how past online behaviours could impact on their future, when applying for a place at university or a job for example.
- discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with
- asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

How and when to seek support

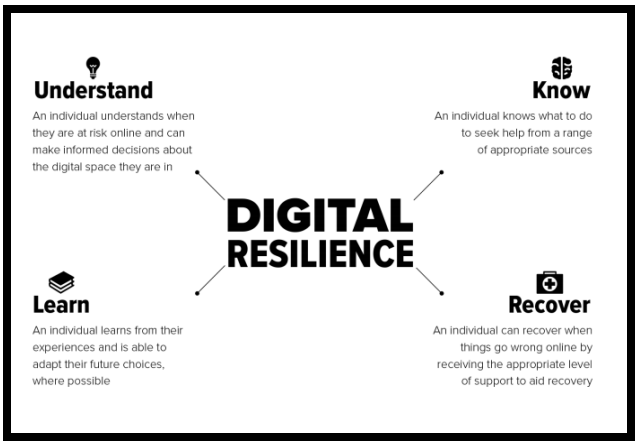
We enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online through

- helping them to identify who trusted adults are
- looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline

- helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

Digital Resilience

Resilience can be defined as 'a process to harness resources to sustain wellbeing', and digital resilience as the application of this concept to technology, the internet and the digital age. Digital resilience helps individuals recognise and manage the risks they come across when they socialise, explore or work online. It is achieved primarily through experience, rather than learning and it is fostered by opportunities to confide in trusted others and later reflect upon online challenges. We teach the children to adhere to the following digital resilience model.



Wellbeing

We enable pupils to understand how online behaviors can impact on their wellbeing:

- Self-image and identity
- Online reputation
- Online bullying
- Health, wellbeing and lifestyle

This includes knowing about the impact of comparisons to 'unrealistic' online images, knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent on and offline, people can often behave differently online to how they would act face to face, what users post can affect future career opportunities and relationships – both positively and negatively.

Use of external visitors

Due to the ever-changing nature of the online world, it is increasingly difficult to keep up to date with the many trends. For this reason, and to enhance our curriculum offer, we regularly invite 'experts' in to deliver engaging and useful online safety messages to the children, parents and staff.

A Whole School Approach

We deliver a whole-school approach that goes beyond individual lessons. It includes all aspects of school life, including culture, ethos, environment and partnerships with families and the community. In St. Edward's we

- Create a culture that incorporates the principles of online safety across all elements of school life which are reflected in the school's policies and practice and should be communicated with staff, pupils and parents.
- Proactively engage staff, pupils and parents/carers in school activities that promote the agreed principles of online safety.
- Develop Digital Champions who provide peer-to-peer support.
    - Embed the online safety principles when teaching curriculum subjects and other teaching opportunities and reinforcing what is taught in lessons by taking appropriate and consistent action when a pupil makes a report of unacceptable online behaviours from another pupil, including cyberbullying, or shares a concern about something they have seen online.
- Model the online safety principles consistently by expecting the same standards of behaviour whenever a pupil is online at school. This support is also extended to parents, so they are able to incorporate the same principles of online safety at home.

Managing Internet Access

Information system security

The security of school ICT systems will be reviewed regularly. Virus protection (presently through one IT) will be updated regularly. Security strategies will be discussed with the ICT support team. Files held on the school network will be checked regularly. The use of logins and passwords for staff and pupils to access the school network will be enforced.

Published content, social media and the school web site

Staff or pupil personal contact information will not be published. Our contact details given online will be via the school office.

Any photographs including staff members will carefully selected so that images cannot be misused. Group photographs should be used rather than photographs of individuals. Full-face photos of individual staff members should not be used. Staff names should not be published.

The Executive Headteacher, Head of School, Senior Management Team (SLT) and the online safety lead will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully to reduce the risk of images being reused or misused. Ideally, group photographs should be used rather than photographs of individual children.

Full names will not be used anywhere on a school web site, social media or other on-line space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. This information will be shared with all staff.

Pupil images or file names will not refer to the pupil by name.

Pupil work will not refer to the child's full name – only first names will be used and for most situations work can remain anonymous.

Parents should be clearly informed of the school policy on photograph taking or videos and their publication, both on school and independent electronic repositories. This must be updated annually.

Social networking and personal publishing

The school will restrict access to social networking sites on school computers and consider how to appropriately educate pupils in their safe use. This will largely depend on the risks posed by particular social media applications the pupils are accessing at home. The only recommended social networking personal publication site is Twitter.

Pupils will be advised *never* to give out personal details of any kind, which may identify themselves, their friends or their location.

Pupils and parents will be educated that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Concerns regarding students' use of social networking, social media and personal publishing sites (out of school) will be raised with their parents/carers, particularly when concerning students' inappropriate use.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

Managing filtering

The school will work with One IT to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the online safety lead, the headteacher or member of the SLT.

Senior staff (with the support of one IT) will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

Any videoconferencing should use our educational broadband network (NGfL) to ensure quality of service and security. Pupils must ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing and webcam use will be appropriately supervised for the pupil's age and ability.

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.

Pupils will be instructed about safe and appropriate use of personal devices.

The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones will not be used during lessons or formal school time. The school will take steps to ensure that children do not use mobile phones on school premises or in connection with school activities. Pupils would do need to bring personal devices onto school property (for safety reasons, such as walking home alone) must sign them in at the school office in the morning and collect them at home time, in usual circumstances. During COVID-19 restrictions, class teachers will keep mobile phones in a box in a safe place within their classroom (e.g. within a cupboard).

Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. They should not be used in school or any other officially sanctioned location.

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

Preventing radicalisation and extremism
The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content. We also filter out social media, such as Facebook. Searches and web addresses are monitored and the ICT technician (One IT) will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.

Where staff, students or visitors find unblocked extremist content they must report it to a senior member of staff.

As part of the Computing curriculum, pupils are taught how to stay safe online, both in school and outside. This is also embedded into our PSHE and SMSC curriculum.

The Acceptable User ICT Policy (AUP) refers to preventing radicalisation and related extremist content. Pupils and staff are asked to sign the AUP annually to confirm they have understood what is acceptable. Pupils and staff know how to report internet content that is inappropriate or of concern.

Signs of vulnerability
There are no known definitive indicators that a young person is vulnerable to radicalisation, but there are number of signs that together increase the risk. Signs of vulnerability include:

- underachievement
- being in possession of extremist literature
- poverty
- social exclusion
- traumatic events
- global or national events
- religious conversion
- change in behaviour
- extremist influences
- conflict with family over lifestyle

- confused identify
- victim or witness to race or hate crimes
- rejection by peers, family, social groups or faith

Recognising Extremism
Early indicators of radicalisation or extremism may include:

- showing sympathy for extremist causes
- glorifying violence, especially to other faiths or cultures
- making remarks or comments about being at extremist events or rallies outside school
- evidence of possessing illegal or extremist literature
- advocating messages similar to illegal organisations or other extremist groups
- out of character changes in dress, behaviour and peer relationships (but there are also very powerful narratives, programmes and networks that young people can come across online so involvement with particular groups may not be apparent.)
- secretive behaviour
- online searches or sharing extremist messages or social profiles
- intolerance of difference, including faith, culture, gender, race or sexuality
- graffiti, art work or writing that displays extremist themes
- attempts to impose extremist views or practices on others
- verbalising anti-Western or anti-British views
- advocating violence towards others

Referral Process
Staff and visitors to the school must refer all concerns about children and young people who show signs of vulnerability or radicalisation to the Designated Safeguarding Lead using the usual methods for reporting other safeguarding concerns. When there are significant concerns about a pupil, the Designated Safeguarding Lead in liaison with the Executive Headteacher/Head of School will make a referral to the appropriate body.

Social Media Platforms
Social media has become an essential and exciting part of how we live. Millions of young people use these platforms daily to share content. However, there are a small

minority of users who exploit social media to radicalise and recruit vulnerable people. The government and police work closely with the communications industry to remove extremist, criminal and terrorist content from the internet.

Policy Decisions

Authorising Internet access

All staff (including supply staff) must read and sign our Acceptable Use Policy before using any school ICT resource.

Parents will be asked to sign and return an Acceptable Use consent form annually in respect of their child/children. Children will also be asked to sign this form.

At Key Stage 1 and in Foundation Stage, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher directed where necessary.

Any person not directly employed by the school will be asked to sign an Acceptable Use agreement before being allowed to access the Internet from the school site.

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. The school cannot accept liability for any material accessed, or any consequences of Internet access. Any unsuitable material that does appear on the school network, should be immediately reported to the online safety coordinator to allow for the site to be blocked.

We will regularly audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

Handling online safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Head of School/Executive Headteacher.

The online safety lead will record all reported pupil incidents and actions taken on CPOMs.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure (see schools complaints policy)

Pupils and parents will be informed of consequences for pupils misusing the Internet *through our Acceptable User Agreement.*

Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986.

Cyberbullying of any member of the school community will not be tolerated (details of bullying procedure are handled in the school behaviour policy)

All incidents of cyberbullying reported to the school will be recorded.

There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate OR
- A service provider (schools) may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time.
- Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.

Communications

Introducing the online safety policy to pupils
Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and any misuse will be followed up.

- *A programme of training in e-Safety will be developed, based on the materials from CEOP.*

- *Online Safety training will be embedded within the computing curriculum as a key strand or the Personal Social and Health Education (PSHE) curriculum.*

- *The school supports the international Safer Internet Day each February, provides opportunities for pupils to consider cyberbullying as part of Anti-Bullying week in the autumn term and considers age-appropriate and healthy use of technology during Health week in the summer term.*

Particular attention to online safety education will be given where pupils are considered to be vulnerable.

Staff and the Online Safety Policy
All teaching and support staff will be given the School Online Safety Policy and its importance explained.

Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use (Computing Lead and Local Technician) will be supervised by senior management and work to clear procedures for reporting issues.

Up to date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

Where possible staff will use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents and carer's attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.

The school will maintain a list of online safety resources for parents/carers, which are also published on the school website.

Useful online Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Orange Education: www1.orange.co.uk/education
- Safe: www.safesocialnetworking.org
- CEOP: https://www.ceop.police.uk/safety-centre/

The school will ask all new parents to sign the acceptable use agreement when they register their child with the school. These will be updated by all parents/pupils on an annual basis.

Issues arising from home use of Internet and social networking

- Involve parents – raising awareness opportunities
- Consideration be given to reporting underage social network accounts in the event of abuse.

Next Review: September 2021

Associated documents

- Internet Policy and Letter
- Responsible User Agreement Policy
- Use of Photos and Videos Policy
- Computing Policy
- Safeguarding policy
- PSHE Policy
- Keeping Children Safe in Education (DfE, 2020)
- Education in a Connected World (UKCIS, 2018)
- Teaching Online Safety in School (DfE, June 2019)
- Digital Resilience Framework (UKCIS, 2019)