



ONLINE SAFETY & ACCEPTABLE USE POLICY

(Safeguarding • Digital Citizenship • Data Protection • AI • Cyber Security)

We are a school family journeying together in God's love.
We serve each other to achieve our best.
We learn in fun and creative ways,
respecting everyone's gifts.

Policy information	Details
Policy status	School safeguarding / online safety policy
Effective from	September 2026
Review date	September 2027, or sooner if guidance changes
Policy lead	Headteacher / Online Safety Lead
Designated Safeguarding Lead	Mrs Snell
Online Safety Lead / ICT Subject Leader	Mrs Snell / Ms McGimpsey
Safeguarding Governor	Julie Bullock

Contents

- 1. Introduction and purpose
- 2. Policy aims
- 3. Legislation and national guidance
- 4. Related school policies
- 5. Scope
- 6. Roles and responsibilities
- 7. Teaching and learning
- 8. Artificial intelligence
- 9. Filtering and monitoring
- 10. Searching, screening and confiscation
- 11. Email and digital communication
- 12. Social media
- 13. Digital photography, video and audio
- 14. Mobile phones and personal devices
- 15. Cyber security
- 16. Data protection
- 17. Online bullying
- 18. Online sexual harassment, abuse and exploitation
- 19. Radicalisation and extremism
- 20. Misinformation, disinformation and deepfakes
- 21. Responding to incidents
- 22. Staff training
- 23. Parents and carers
- 24. Remote/home learning
- 25. Monitoring and review
- 26. Breaches and sanctions
- 27. Catholic ethos and online safety
- Appendix 1: Staff AUP
- Appendix 2: Pupil AUP
- Appendix 3: Quick reporting flow

Online safety is connected to the dignity and worth of every person. Children are taught that their online behaviour should reflect respect, compassion, honesty, responsibility and care for others.

Catholic Social Teaching principles, including human dignity, the common good and solidarity, inform the school's approach to digital citizenship. Children are encouraged to ask: "Is it true? Is it kind? Is it respectful? Is it safe? Is it something I would be happy for others to see?"

1. Introduction and purpose

New and emerging technologies provide significant opportunities for children to learn, communicate, collaborate and create. Digital technology is an integral part of children's lives both within and beyond school.

St Edward's Catholic Primary School recognises the educational, social and cultural benefits of technology while also recognising risks including inappropriate or harmful content, online bullying, grooming, exploitation, abuse, misinformation, disinformation, loss of privacy, scams, excessive screen use, inappropriate communication, online sexual harassment and misuse of artificial intelligence.

As a Catholic school, we seek to develop children who use technology responsibly, respectfully and wisely, recognising the dignity of every person and their responsibility towards others. Online safety is therefore a safeguarding responsibility and an integral part of the curriculum, pastoral provision and wider personal development.

2. Policy aims

The school aims to protect children and adults from digital risks; promote safe, responsible and respectful use of technology; provide clear expectations for all users; support safeguarding; maintain effective filtering and monitoring; teach children to recognise risks and seek help; promote digital literacy and critical thinking; protect personal information; provide appropriate safeguards around AI; and work in partnership with parents and carers.

3. Legislation and national guidance

This policy should be read alongside current statutory guidance including Keeping Children Safe in Education 2026 and Working Together to Safeguard Children 2026, together with the Children Acts 1989 and 2004, Education Act 2011, Equality Act 2010, Data Protection Act 2018, UK GDPR and applicable provisions of the Data Use and Access Act 2025.

The school will also have regard to current DfE guidance on filtering and monitoring, generative AI in education, AI product safety, data protection, Prevent and cyber security, together with relevant UK Council for Internet Safety, CEOP and Internet Watch Foundation resources. References will be reviewed when national guidance changes.

4. Related school policies

This policy should be read with the Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Staff and Pupil Acceptable Use Agreements, Data Protection and Privacy Policy, Social Media and Digital Photography Policy, Mobile Phone Policy, Remote/Distance Learning Policy, RSE/RSHE Policy, Inclusion/SEND Policy, Prevent procedures, Whistleblowing Policy, Complaints Policy and Cyber Security procedures.

5. Scope

This policy applies to pupils, staff, governors, volunteers, supply and agency staff, contractors and visitors using school-owned, school-managed or school-approved digital systems. It applies in school, on visits, during clubs, remote learning and when school systems or personal devices are used for school-related purposes.

6. Roles and responsibilities

Governors: approve and review the policy, provide challenge and assurance, and receive appropriate information about safeguarding, filtering and monitoring.

Headteacher: has overall responsibility for safeguarding, ensures implementation, training, appropriate filtering/monitoring and safe adoption of new technologies.

DSL – Mrs Snell: manages online safeguarding concerns, CPOMS recording, referrals and liaison with families and external agencies.

Online Safety Lead / ICT Subject Leader – Mrs Snell with Ms McGimpsey as subject lead, coordinate day-to-day online safety, staff advice, curriculum provision, incident information and liaison with technical support.

Technical support: 'ONETEC' maintains agreed filtering, monitoring, network security, updates, logs and technical incident response.

All staff and volunteers: follow this policy and the AUP, maintain professional boundaries, supervise pupils, protect data and report concerns promptly.

Pupils: use technology respectfully, keep passwords secure, follow school rules, report concerns and use AI only where specifically permitted and supervised.

7. Teaching and learning

Online safety is embedded throughout the curriculum. Age-appropriate teaching covers privacy, passwords, online relationships, cyberbullying, gaming, social media, scams and phishing, advertising, digital footprints, image sharing, grooming and exploitation, online sexual harassment, radicalisation, misinformation, copyright, healthy technology use and AI.

Children are taught that not everything online is true and that information should be checked critically. The school will promote Safer Internet Day and other appropriate whole-school activities. Staff will model safe and responsible digital behaviour.

8. Artificial intelligence

The school adopts a safety-first approach to AI. Staff may only use school-approved AI tools and must not enter confidential, safeguarding or personally identifiable pupil information into public or unapproved systems. Photographs of pupils must not be uploaded to AI services unless specifically authorised and compliant with data protection arrangements.

Staff must check AI outputs for accuracy, bias, inappropriate content and copyright issues. AI must not replace professional judgement.

Primary-aged pupils will not independently use generative AI unless the tool is approved, age appropriate, educationally justified and supervised. Children will learn that AI can make mistakes, can generate misleading content and must never be given unnecessary personal information. AI may support learning but should not replace children's own thinking, creativity or work.

9. Filtering and monitoring

The school will maintain appropriate filtering and monitoring in line with the current DfE digital and technology standards. Arrangements will be proportionate to the school's context and regularly reviewed.

The school will review filtering and monitoring reports, ensure alerts are appropriately escalated to the DSL, review blocked and allowed categories, maintain relevant records and respond to emerging threats.

Filtering prevents access to illegal, inappropriate or harmful content; monitoring provides an additional safeguarding layer. Neither replaces effective teaching, supervision or professional judgement.

If potentially illegal material is encountered, users must not download, save, copy or forward it. It must be reported immediately to the DSL/Headteacher and technical lead.

10. Searching, screening and confiscation

The school will follow current legal powers and national guidance when searching pupils or confiscating prohibited items. Where there is reasonable cause to believe that a device contains evidence of a criminal offence, harm, bullying, serious disruption or breach of school rules, staff may act in accordance with the Behaviour Policy and safeguarding procedures.

Where material may constitute evidence of a criminal offence or serious safeguarding concern, the Headteacher/DSL will seek appropriate advice from the Police or other agencies. Staff should avoid unnecessary viewing, copying or distribution of illegal material.

11. Email and digital communication

Staff will use approved school accounts and platforms, maintain professional language and communicate with pupils and parents/carers only through approved systems. Personal email and private messaging must not be used for pupil communication.

Pupils will be taught to communicate respectfully, protect passwords, recognise suspicious links and report inappropriate or concerning messages.

12. Social media

Staff must maintain professional boundaries online. They must not privately communicate with pupils through personal social media or messaging accounts, publish confidential school information, or post material that could compromise their professional responsibilities.

The Social Media and Digital Photography Policy applies to staff, pupils and relevant members of the school community.

13. Digital photography, video and audio

Images and recordings will be made only for legitimate school purposes and handled securely. Appropriate consent will be obtained where required. School-approved equipment should be used wherever possible. Personal devices must not be used to store pupil images unless specifically authorised. Images must not be shared through personal accounts.

14. Mobile phones and personal devices

The Mobile Phone Policy and Social Media and Digital Photography Policy apply. Personal devices must not compromise safeguarding, confidentiality or professional boundaries. Staff must secure devices appropriately and must not photograph or record pupils without authorisation.

15. Cyber security

All users must protect school systems by keeping passwords confidential, using strong passwords and multi-factor authentication where provided, locking devices when unattended, reporting lost or stolen devices, identifying phishing, avoiding unauthorised software and never bypassing security controls.

Suspected malware, ransomware, compromised accounts, phishing attacks or significant data breaches must be reported immediately to the Headteacher, appropriate technical support and DPO.

16. Data protection

Personal information must be processed in accordance with UK data protection law and the school's Data Protection Policy. It must be lawful, fair, transparent, necessary, accurate, securely stored and retained appropriately.

Particular care is required with safeguarding, SEND, medical, staff, parental and image data. Personal data must not be entered into public or unapproved AI systems. Suspected data breaches must be reported immediately to the DPO.

17. Online bullying

Cyberbullying includes threatening or abusive messages, exclusion from online groups, rumours, embarrassing images, impersonation, fake accounts and harassment through gaming or messaging platforms.

Reports will be taken seriously. The school will listen, establish facts, record concerns, assess safeguarding risk, involve parents/carers where appropriate, take proportionate action, provide support and monitor the situation.

18. Online sexual harassment, abuse and exploitation

The school recognises online sexual harassment and abuse may include sexualised comments, unwanted sexual messages, pressure to send images, image-based abuse, grooming, coercion, exploitation and digitally altered sexualised images.

All concerns must be reported immediately to the DSL and managed under safeguarding procedures. Staff must not promise confidentiality. Where appropriate, the school will seek advice from Children's Social Care, Police, CEOP or other agencies.

19. Radicalisation and extremism

Children may encounter extremist or radicalising content online. Staff must report concerns through safeguarding procedures. The school will fulfil its Prevent responsibilities and teach children, in an age-appropriate way, to question information, recognise manipulation and seek help.

20. Misinformation, disinformation and deepfakes

Children will learn that digital content can be inaccurate, deliberately misleading, manipulated or AI-generated. They will develop skills to check sources, compare information, identify trustworthy sites, question suspicious claims and recognise manipulated images and videos.

21. Responding to incidents

All concerns must be reported promptly. The response may include immediate safeguarding action, DSL/Headteacher involvement, CPOMS recording, parent/carers contact where appropriate, technical investigation, preservation of evidence, referral to Children's Social Care, Police, CEOP or Prevent channels, disciplinary action and support for those affected.

Children should be involved in decisions affecting them wherever appropriate. Staff must not unnecessarily forward inappropriate images or content.

22. Staff training

Online safety training forms part of safeguarding training and induction. Training will address filtering and monitoring, cyber security, phishing, online grooming and exploitation, sexual harassment, cyberbullying, radicalisation, AI, data protection, professional boundaries, digital photography and reporting procedures. Staff will receive updates when significant new risks emerge.

23. Parents and carers

The school will provide information about online safety, emerging risks, parental controls, age restrictions and reporting mechanisms. Parents/carers are encouraged to discuss online safety with children and model responsible digital behaviour.

Parents/carers are expected to follow the school's Social Media Code of Conduct. The school will respond where online behaviour has a safeguarding or educational impact on the school community.

24. Remote/home learning

The Remote/Distance Learning Policy applies. Staff will use approved platforms, maintain professional boundaries, protect pupil information and report safeguarding concerns through normal procedures.

25. Monitoring and review

Effectiveness will be evaluated through safeguarding monitoring, CPOMS records, filtering and monitoring reports, staff and pupil voice, parent feedback, curriculum monitoring, governor oversight and technical security reviews. This policy will be reviewed annually and sooner if legislation, technology or safeguarding risks change.

26. Breaches and sanctions

Misuse may result in removal or restriction of access, loss of device privileges, restorative action, parental involvement, disciplinary action, action under the Behaviour Policy, staff disciplinary procedures or referral to external agencies. Where behaviour may constitute a criminal offence, the school may refer to the Police.

Appendix 1 – Staff Acceptable Use Agreement

St Edward's Catholic Primary School

I understand that digital technology is an important part of teaching, learning and school administration and that I have a responsibility to use technology safely, professionally and responsibly.

- I will comply with the school's Online Safety and Acceptable Use Policy, Staff Code of Conduct, safeguarding and data protection policies.
- I will use school-approved systems and keep passwords and authentication information secure.
- I will lock devices when unattended and report compromised accounts, lost devices, phishing, malware or other cyber-security concerns immediately.
- I will not share confidential pupil or school information through unapproved platforms.
- I will not enter safeguarding or personally identifiable pupil information into public or unapproved AI tools.
- I will use only AI tools approved by the school and check AI-generated information for accuracy, bias, appropriateness and copyright.
- I will maintain professional boundaries and communicate with pupils and parents/carers only through approved school systems.
- I will not privately message pupils using personal social media or messaging accounts.
- I will follow school requirements for photography, video and recording and will not use personal devices to store pupil images unless specifically authorised.
- I will not bypass filtering or security systems or install unauthorised software.
- I will report illegal, inappropriate or concerning material immediately and will not unnecessarily copy or forward it.
- I will respect copyright and intellectual property.
- I understand that use of school systems may be monitored and that this agreement applies when using school systems away from school.
- I understand that misuse may result in disciplinary action and, where appropriate, referral to external agencies.

Name	
Position	
Signature	
Date	

Appendix 2 – Pupil Online Safety Agreement

At St Edward's Catholic Primary School, I agree that I will:

- be kind and respectful online;
- keep my passwords private;
- ask permission before using technology when required;
- only use websites, apps and games that my teacher says are appropriate;
- never deliberately look for inappropriate material;
- tell an adult if something online worries, frightens or upsets me;
- never share personal information about myself or someone else;
- never take or share photographs or videos of others without permission;
- never use technology to bully, threaten or hurt someone;
- remember that things I post online can have consequences;
- check information before believing or sharing it;
- understand that AI can make mistakes and never give personal information to an AI tool;
- use technology to help myself and others learn;
- treat people online with the same dignity and respect I would show them face to face.

Pupil name	
Class	
Signature	
Date	

Appendix 3 – Quick Online Safety Reporting Flow

1. 1. STOP – Do not reply, forward, copy or save harmful/illegal content unnecessarily.
2. 2. REPORT – Tell a teacher, trusted adult, DSL or other designated staff member immediately.
3. 3. RECORD – The concern is recorded factually on CPOMS or the approved school safeguarding system.
4. 4. ESCALATE – The DSL/Headteacher decides whether technical support, parents/carers, Children's Social Care, Police, CEOP or Prevent should be contacted.
5. 5. SUPPORT – The child/adult affected is supported and the situation is monitored.
6. 6. REVIEW – The school considers whether curriculum, filtering, monitoring, training or policy changes are needed.