St Vincent's Catholic Primary School

Online Safety Policy

Title	Online Safety Policy
Policy Approval	October 2026
Policy Review	October 2027

Let your light shine

Be Passionate about Learning

Be Kind

Be Respectful

Make a Difference

Our Mission Statement

"Let your light shine"

Jesus said "I am the light of world whoever follows me will have the light of life."

Our Values

We are passionate about learning

We are kind

We are respectful

We make a difference

Online Safety Policy

St Vincent's Catholic Primary School

UNICEF Rights Respecting School Principles

As a UNICEF Rights Respecting Gold Award School, we uphold children's rights in all aspects of school life, including online safety.

In particular, we recognise:

- **Article 17** – Children have the right to access information that supports their wellbeing and development.
- **Article 19** – Children have the right to be protected from harm, abuse and exploitation.
- **Article 3** – The best interests of the child must be a primary consideration in all decisions affecting them.
- **Article 12** – Children have the right to be listened to and have their views taken seriously.

We promote these rights by teaching pupils how to use technology safely, responsibly and respectfully, while ensuring they are protected from online risks and know how to seek help if they have concerns.

Policy Statement

St Vincent's Catholic Primary School recognises the significant role that the internet, digital technology and online communication play in the lives of children, families and staff. Technology provides valuable opportunities for learning, creativity, communication and personal development. However, we are equally committed to protecting children, staff and families from potential online risks and ensuring the safe, responsible and positive use of digital technology.

This policy forms part of our wider safeguarding arrangements and should be read alongside the school's Safeguarding and Child Protection Policy, Acceptable Use Policy, Staff Code of Conduct and Data Protection Policy.

We refer to the following guidance and standards to support the development and implementation of this policy:

- Keeping Children Safe in Education (KCSIE)
- Teaching Online Safety in Schools
- Meeting Digital and Technology Standards in Schools and Colleges: Filtering and Monitoring Standards

- Generative Artificial Intelligence (AI) in Education
- Guidance published by the UK Council for Internet Safety (UKCIS) and the UK Safer Internet Centre where appropriate.
- Safeguarding children and protecting professionals in early years settings: online safety considerations, where applicable.

This policy applies to all staff, governors, volunteers, students, visitors, parents/carers and pupils using digital technologies in relation to St Vincent's Catholic Primary School. It covers all school-owned devices, systems and online platforms, as well as personal devices used on school premises where applicable.

Aims and Objectives

Our aims are to:

- Safeguard children from potential harm arising from online activity or exposure to inappropriate content.
- Support staff to use digital technology safely, responsibly and professionally.
- Develop pupils' understanding of online safety and responsible digital citizenship.
- Work in partnership with parents and carers to reinforce online safety messages both in school and at home.

The Designated Safeguarding Lead (DSL) is ultimately responsible for online safety concerns. All concerns should be raised as soon as possible with **Anita Harrop**.

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation, with technology often providing the platform that facilitates harm.

The breadth of issues included within online safety is considerable but can be categorised into four areas of risk.

Content

Being exposed to illegal, inappropriate or harmful material, such as:

- Pornography
- Fake news
- Racism

- Misogyny
- Self-harm
- Suicide
- Antisemitism
- Radicalisation and extremism
- Misinformation and disinformation
- Conspiracy theories
- Deepfake images, videos and audio
- Manipulated online content designed to deceive or exploit users

Contact

Being subjected to harmful online interaction with other users, such as:

- Child-on-child pressure
- Commercial advertising
- Adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes

Conduct

Personal online behaviour that increases the likelihood of, or causes, harm, such as:

- Making, sending or receiving explicit images
- Consensual and non-consensual sharing of nude or semi-nude images
- Sharing other inappropriate content
- Online bullying and harassment
- The creation or sharing of misleading AI-generated content
- The misuse of artificial intelligence tools
- The creation, sharing or use of digitally altered images or videos to harm, embarrass or exploit others

Commerce

Risks such as:

- Online gambling

- Inappropriate advertising
- Phishing
- Financial scams

How We Keep Children Safe

Children are taught age-appropriate online safety concepts through the curriculum, assemblies, discussions, themed events and educational resources. Online safety education is embedded within Computing, PSHE and Relationships Education and reinforced across the wider curriculum.

Within school we aim to keep pupils, staff and parents safe online through the following measures:

- Ensuring appropriate antivirus and anti-spyware software is installed and regularly updated on all devices.
- Ensuring content filters and web-monitoring systems are in place on all school devices.
- Ensuring all devices are password protected and have appropriate screen-lock settings.
- Reminding staff to use strong passwords, keep them secure, change them regularly and never share them with others.
- Monitoring internet usage across the school network.
- Providing secure storage of all school-owned devices when not in use.
- Ensuring social media and messaging applications are only installed where required for legitimate educational or operational purposes and have been approved by school leaders.
- Reviewing all applications and software used within school to ensure they are appropriate for pupils' age and educational needs.
- Using only approved school devices to photograph, record or store information relating to pupils.
- Never emailing personal or financial information unless through approved secure methods.
- Reporting online content that is illegal or harmful to the Internet Watch Foundation (IWF) where appropriate.

- Teaching pupils how to stay safe online and how to report concerns.
- Ensuring pupils are appropriately supervised when using internet-connected devices.
- Using monitoring software and filtering systems to support safe internet use.
- Teaching pupils how to identify trusted adults and recognise situations where they should seek help.
- Discussing safe use of online communication platforms such as Microsoft Teams and other approved educational platforms where applicable.
- Providing annual online safety training for all staff.
- Ensuring staff model safe and responsible technology use and adhere to the school's Acceptable Use Policy.
- Monitoring and managing screen time within teaching and learning activities to ensure it supports educational outcomes and pupil wellbeing.
- Considering the physical safety and wellbeing of users when working with technology, including posture and ergonomics.
- Being aware of the need to manage our digital reputation, including information posted online both professionally and personally.
- Ensuring staff do not communicate with parents or pupils through personal social media accounts or personal messaging services.
- Ensuring all electronic communication between staff and parents/carers takes place through approved school communication channels.
- Signposting parents and carers to appropriate online safety information and support.
- Teaching pupils how to critically evaluate online information and identify misinformation, disinformation and manipulated content.
- Raising awareness of emerging online risks, including AI-generated content, deepfakes and online scams.
- Providing additional support where necessary for pupils who may be more vulnerable online, including pupils with SEND, communication difficulties or identified safeguarding concerns.
- Reminding pupils regularly how and where they can report online safety concerns and seek support.

- Ensuring that where personal devices are permitted, appropriate safeguards, supervision and expectations are in place.

Artificial Intelligence (AI)

The school recognises the increasing use of artificial intelligence (AI) and generative AI technologies within education and wider society. The Department for Education now expects schools to consider the safeguarding implications of AI technologies, including when reviewing filtering and monitoring systems.

While AI presents opportunities to support teaching, learning and administration, it also introduces safeguarding, privacy and online safety risks.

The school will:

- Ensure any AI tools used by staff or pupils are appropriately assessed for safeguarding, privacy and educational suitability.
- Consider the risks of inaccurate, misleading or harmful AI-generated content.
- Teach pupils to think critically about information generated by AI systems.
- Promote responsible and ethical use of AI technologies.
- Ensure staff understand the limitations of AI and exercise professional judgement when using AI-generated content.
- Consider AI-related risks as part of online safety education and safeguarding procedures.
- Ensure that the use of AI complies with UK GDPR, data protection requirements and relevant Department for Education guidance.
- Review filtering and monitoring arrangements to ensure they remain effective as AI technologies develop.

Responsibilities of All Staff

All staff, including supply staff, contractors, volunteers and governors, are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing to and adhering to the school's Acceptable Use Policy.

- Knowing that the DSL is responsible for filtering and monitoring systems and understanding how to report concerns regarding these systems.
- Following correct procedures when authorised access is required to bypass filtering systems for educational purposes.
- Working with the DSL to ensure all online safety incidents are logged and dealt with appropriately.
- Ensuring any incidents of cyberbullying are managed in accordance with the school's Behaviour Policy and Staff Code of Conduct.
- Responding appropriately to concerns about sexual violence and sexual harassment, both online and offline, while maintaining an attitude that "it could happen here".
- Maintaining professional standards when using digital technology and online communication.

This list is not intended to be exhaustive.

Filtering and Monitoring

The Governing Body, Headteacher, Designated Safeguarding Lead and relevant technical staff will work together to ensure that filtering and monitoring systems remain effective and appropriate for the age, needs and risks of pupils within the school.

The school will:

- Ensure clear leadership responsibility for filtering and monitoring systems.
- Undertake and document a review of filtering and monitoring arrangements at least annually.
- Consider emerging risks, including artificial intelligence, personal devices and changes in technology.
- Consider the needs of vulnerable pupils, including pupils with SEND, when reviewing filtering and monitoring arrangements.
- Ensure staff know how to report concerns regarding filtering and monitoring systems.

Acceptable Use of the Internet

All staff, governors, volunteers and visitors are expected to read and agree to the school's Acceptable Use Policy where relevant.

Use of the school's internet and digital systems must be for educational purposes, professional responsibilities or approved school business only.

The school monitors internet usage, where appropriate, to ensure compliance with this policy and will restrict access to inappropriate material through filtering and monitoring systems.

Responding to Concerns

If concerns arise relating to online safety, the school will follow its Safeguarding and Child Protection Policy and report concerns to the Designated Safeguarding Lead.

The DSL will ensure that:

- All staff understand how to report concerns and when concerns should be escalated.
- All incidents are logged, assessed and actioned in accordance with safeguarding procedures.
- Parents/carers are supported in developing their knowledge and understanding of online safety issues.
- Parents/carers are offered guidance and resources to support discussions about online safety at home.
- Families are signposted to reliable sources of online safety support and advice.
- Staff have access to relevant online safety information and professional guidance.
- Appropriate records are maintained regarding online safety incidents.

Online safety concerns may arise both within and outside school. Any concern that indicates a child may be at risk of harm will be treated as a safeguarding concern and managed in accordance with the Safeguarding and Child Protection Policy. Staff will maintain an attitude that “it could happen here” when responding to online safety concerns.

Under no circumstances should any member of staff, either at work or elsewhere, make, deliberately download, possess or distribute material known to be illegal, including child sexual abuse material.

The DSL will consider whether incidents involving illegal activity, serious safeguarding concerns or criminal offences should be referred to the police, children's social care or other relevant agencies.

Cyber Security

Good cyber security means protecting the personal and sensitive information that we hold about pupils, staff and families in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The school recognises that cyber criminals may target educational settings and is committed to ensuring all staff understand the importance of protecting the information we hold.

All staff are expected to follow school procedures relating to data protection, secure storage, password management and the safe use of technology.

We Will:

- Use strong passwords that are updated regularly for all digital systems.
- Restrict access to data and systems on a "need to know" basis.
- Ensure antivirus protection, firewalls and software updates are maintained on all devices.
- Store backups securely and test them regularly.
- Protect online accounts using multi-factor authentication wherever possible.
- Use secure, encrypted connections for data transfers and communications.
- Report suspected data breaches immediately to the Headteacher and DSL, who will follow the school's data breach procedures.
- Provide regular cyber security awareness training for staff, including recognising phishing emails, password security and avoiding malicious links.
- Ensure staff complete regular cyber security awareness training.
- Regularly review access permissions to school systems and online platforms.
- Ensure all software, operating systems and security updates are applied promptly.
- Consider cyber security risks when introducing new technologies, applications or AI tools.

To prevent potential data breaches that could disrupt school operations and compromise sensitive information, staff are reminded not to open suspicious emails or messages relating to matters such as:

- Password resets
- Compensation claims
- Device scanning alerts
- Missed deliveries
- Unexpected invoices or payment requests

Staff must report any suspicious communications immediately to the Headteacher or School Business Manager.

Suspected phishing emails should also be reported to the National Cyber Security Centre Suspicious Email Reporting Service at:

report@phishing.gov.uk

Monitoring and Review

This policy will be reviewed annually, or sooner if required, to reflect:

- Changes in legislation or statutory guidance.
- Updates to safeguarding requirements.
- Emerging technologies and online risks.
- Developments in filtering, monitoring and cyber security standards.

The review will involve the Headteacher, Designated Safeguarding Lead, Governors and relevant technical staff where appropriate.

Policy Review Cycle: Annual
Approved by: Governing Body
Next Review Date: September 2027 (or sooner if statutory guidance changes)