St John Vianney
Catholic Primary School



"Seeking Growth Together"

E-Safety and Internet Access Policy

Date Reviewed: September 2026
Reviewed by: School Business Lead
Approved by Headteacher
Date of next review: September 2027

1. Purpose and aims

St John Vianney Catholic Primary School is committed to helping every pupil use technology safely, respectfully, responsibly and confidently. Online safety is a safeguarding responsibility and an essential part of our computing, relationships and health education, and wider curriculum provision.

- protect pupils, staff, governors, volunteers and visitors when using digital technology
- teach pupils the knowledge, skills and values needed to make safe and informed choices online
- identify, report and respond promptly to online safety concerns and incidents
- maintain secure systems, appropriate filtering and effective monitoring
- work in partnership with parents and carers to promote consistent online safety messages at home and school
- ensure that the use of artificial intelligence and emerging technologies is safe, ethical and age appropriate

Catholic ethos: Our approach reflects the dignity of every person, the importance of truth, kindness and responsible stewardship, and our mission of Seeking Growth Together through Jesus.

2. Scope

This policy applies to all members of the school community, including pupils, staff, governors, volunteers, contractors, visitors, parents and carers, and community users. It covers school-owned and personal devices, school networks and cloud services, and online behaviour outside school where it affects the welfare of a pupil, a member of staff, the school community or the orderly running of the school.

3. Policy framework

This policy should be read alongside the school's Safeguarding and Child Protection Policy, Behaviour and Relationships Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy, Prevent Policy, Artificial Intelligence Policy, Acceptable Use Policies, Mobile Phone and Camera Policy, and disciplinary and complaints procedures.
It is informed by Keeping Children Safe in Education 2026, the Department for Education digital and technology standards, the Prevent duty, UK GDPR and the Data Protection Act 2018, the Computer Misuse Act 1990, and relevant education and safeguarding legislation.

4. Roles and responsibilities

4.1 Governing Body

- approves this policy and holds leaders to account for its effective implementation
- ensures appropriate filtering and monitoring systems are in place and reviewed at least annually
- receives information about online safety, safeguarding trends, incidents, training and improvement actions
- ensures governors receive appropriate online safety and safeguarding training

4.2 Headteacher and senior leaders

- establish a culture in which online safety is understood as part of safeguarding
- ensure staff understand their responsibilities and receive appropriate induction, training and updates

- ensure serious concerns and allegations are managed under safeguarding, low-level concern, disciplinary or whistleblowing procedures as appropriate
- ensure the school's response to incidents is timely, proportionate, child-centred and properly recorded

4.3 Designated Safeguarding Lead

- has lead responsibility for safeguarding concerns relating to online safety
- ensures online safety is addressed in safeguarding training and curriculum planning
- coordinates referrals and advice from children's social care, the LADO, police or other agencies where required
- reviews relevant monitoring alerts and incident patterns with appropriate leaders

4.4 School Business Lead / Online Safety Lead and technical support

- maintain secure, supported and appropriately configured systems and user accounts
- manage and review filtering, monitoring, cyber security, access controls, backups and software licensing
- ensure there is a clear, auditable process for requesting and approving filtering changes
- report technical breaches, risks and incidents promptly to the Headteacher and DSL
- ensure monitoring is proportionate, transparent and focused on safeguarding, security and acceptable use

4.5 Staff and volunteers

- follow this policy and the relevant Acceptable Use Policy
- use only approved school systems for communication with pupils and parents
- model safe, respectful and lawful use of technology
- supervise pupils' use of technology and plan internet use carefully
- report concerns, accidental access, filtering issues, cyber incidents or suspected misuse immediately
- never investigate suspected illegal content themselves or retain, copy or forward it

4.6 Pupils, parents and carers

- Pupils must follow age-appropriate acceptable use rules and report anything that worries, upsets or confuses them.
- Parents and carers are encouraged to reinforce school messages, supervise online activity appropriately and inform the school of concerns affecting their child or the school community.

5. Online safety across the curriculum

Online safety is taught through a planned, progressive curriculum and reinforced whenever pupils use technology. Teaching is age appropriate, inclusive and responsive to emerging risks and the lived experiences of pupils.

Curriculum strand	Pupils learn about
Self-image and identity	how online activity can shape identity, confidence and reputation
Online relationships	kindness, consent, boundaries, trusted adults and safe communication
Online reputation	digital footprints, permanence and the impact of sharing

Online bullying	recognising, preventing, reporting and responding to harmful behaviour
Managing information	search, reliability, misinformation, disinformation, copyright and plagiarism
Health, wellbeing and lifestyle	screen habits, persuasive design, gaming, sleep and balance
Privacy and security	personal information, passwords, scams, phishing and account security
Copyright and ownership	respecting creators, lawful use and acknowledging sources
Artificial intelligence	how AI-generated content is created, its limitations, bias, accuracy, privacy and responsible use

Teachers will revisit key messages through computing, relationships and health education, English, religious education, assemblies and wider curriculum work. Pupils will be taught to stop, close or move away, tell a trusted adult, preserve appropriate evidence without resharing harmful content, and use reporting or blocking tools where suitable.

6. Filtering, monitoring and technical security

- Internet access on school systems is filtered for all users, with controls appropriate to age, role and educational need.
- School devices and activity are monitored through approved technical and supervisory arrangements. Users are informed that activity may be logged and reviewed.
- Filtering and monitoring arrangements are reviewed at least annually, and sooner following a serious incident, significant system change or new risk.
- The school considers the safeguarding implications of AI-generated and multimodal content when reviewing filtering and monitoring.
- Users must not bypass security, filtering or monitoring, install unauthorised software, use another person's account or share passwords.
- Access rights follow the principle of least privilege. Administrative accounts are limited, protected and separately managed.
- Sensitive data is stored and transferred only through approved secure systems. Personal cloud storage and removable media must not be used for school data unless specifically authorised.

7. Devices, communication, images and AI

7.1 Personal and mobile devices

- Pupils who bring a mobile phone to school must hand it to the school office for secure storage and collect it at the end of the day.
- Pupils may not use personal devices during the school day unless expressly authorised for a specific educational or medical purpose.
- Staff personal phones and smart devices must be stored or used in accordance with the Staff Acceptable Use Policy and must not be used to photograph or record pupils.

- Only approved school devices may connect to school systems and store or process school information.

7.2 Digital communication and social media

- Communication with pupils and parents must use approved school accounts and platforms and remain professional, transparent and appropriate.
- Staff must not use personal accounts, private messaging or personal social media to communicate with pupils.
- Official social media accounts require senior approval, named administrators and appropriate oversight.
- No member of the school community may publish confidential information or content that harms others or brings the school into disrepute.

7.3 Images and recordings

- Images of pupils may be taken only on approved school equipment for an authorised purpose and used in line with consent, data protection and safeguarding requirements.
- Pupils must not take or share images or recordings of others without permission.
- Parents and carers attending school events must respect the privacy and safeguarding of other children and must not publish identifiable images of them without permission.

7.4 Artificial intelligence

- Only school-approved AI tools may be used for school business or pupil-facing activity.
- Personal, confidential, medical, SEND, safeguarding or employment information must not be entered into an AI service unless the service and use have been expressly approved and appropriately protected.
- AI outputs must be checked for accuracy, bias, appropriateness, copyright and safeguarding risks before use.
- Pupils may use AI only within a supervised, planned and age-appropriate curriculum activity.
- AI must support, not replace, professional judgement, teaching, assessment or safeguarding decisions.

8. Reporting concerns and responding to incidents

Anyone who encounters harmful, worrying or inappropriate content or behaviour must report it promptly to a member of staff. Staff must report safeguarding concerns to the DSL without delay and record them through the school's agreed safeguarding system.

Protect	Prioritise the immediate safety and welfare of the child or adult affected.
Report	Inform the DSL and, where relevant, the Headteacher, Online Safety Lead or technical support.
Preserve	Keep proportionate evidence such as URLs, dates, usernames or messages where lawful and safe. Do not copy or view suspected illegal images.

Respond	Follow safeguarding, behaviour, anti-bullying, data breach, disciplinary or emergency procedures as appropriate.
Refer	Seek advice or make referrals to children's social care, LADO, police, CEOP, the Internet Watch Foundation, the DPO or other agencies where required.
Review	Record actions, support those affected, identify lessons and update controls or curriculum provision.

Suspected illegal content: Do not investigate, download, print, copy, forward or repeatedly view it. Stop the activity, secure the device without altering its state where practicable, inform the DSL/Headteacher immediately and seek police or specialist advice.

9. Cyberbullying and harmful online behaviour

Online bullying, harassment, discrimination, impersonation, coercion, harmful sharing and other abusive behaviour will not be tolerated. Incidents will be addressed under the Behaviour and Relationships Policy, Anti-Bullying Policy and safeguarding procedures. The school may act where conduct outside school affects a pupil's welfare, the school community or the orderly running of the school.

- Support will be provided to the child or adult affected.
- Parents and carers will normally be involved where a pupil is affected, unless doing so would increase risk.
- Responses and sanctions will be proportionate to the nature, intent, impact, age and circumstances of the incident.
- Potential criminal conduct or immediate risk will be referred to the appropriate agency.

10. Training, partnership and communication

- All new staff receive online safety, cyber security, data protection and safeguarding information during induction.
- Staff receive at least annual safeguarding and online safety updates, with additional training where roles or risks require it.
- Governors receive appropriate training to support oversight and challenge.
- Pupils receive regular, age-appropriate teaching and reminders, including how to report concerns.
- Parents and carers receive information through the website, newsletters, events and targeted communications where emerging concerns arise.

11. Data protection and confidentiality

- Personal data will be processed lawfully, fairly, transparently and securely in accordance with UK data protection law and school policy.
- Only the minimum necessary information will be collected, used, retained and shared.
- Data breaches or suspected losses must be reported immediately to the Data Protection Officer through the school's agreed procedure.

- School information must not be transferred to personal accounts or devices, or shared with unauthorised individuals.

12. Monitoring and review

The DSL and Online Safety Lead will monitor implementation through incident records, safeguarding information, filtering and monitoring reports, technical audits, curriculum review, training records and feedback from pupils, staff and parents. The Governing Body will receive appropriate assurance information, including anonymised trends and improvement actions.

This policy will be reviewed annually and sooner where there is a significant incident, technological change, identified weakness, or change in statutory guidance or legislation.

Appendix A: Pupil online safety rules

At St John Vianney Catholic Primary School, we use technology to learn, create and communicate. We keep ourselves and others safe by following these rules:

- I use school technology only when a trusted adult has allowed me to.
- I keep passwords and personal information private.
- I am kind, respectful and truthful online.
- I do not take or share images of other people without permission.
- I check information carefully and remember that online or AI-generated content may be wrong or misleading.
- I do not try to bypass filters, change settings or install software.
- If I see something worrying, upsetting or unsafe, I stop and tell a trusted adult immediately.
- I understand that the school may monitor my use of its systems and devices.

Appendix B: Key national guidance

- **Keeping Children Safe in Education 2026:** https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- **DfE filtering and monitoring core standard:** https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard
- **DfE cyber security core standard:** https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard
- **Education for a Connected World:** https://www.gov.uk/government/publications/education-for-a-connected-world
- **UK Safer Internet Centre:** https://saferinternet.org.uk/
- **Childnet:** https://www.childnet.com/
- **CEOP Safety Centre:** https://www.ceop.police.uk/Safety-Centre/

This policy has been developed from the supplied Online Safety Policy content and adapted for St John Vianney Catholic Primary School, with reference to current national guidance available in September 2026.