St John Henry Newman Catholic Primary School

Online Safety Policy

Approved: NOT YET APPROVED

Next Review Date: October 2027

Section 1 – Policy Statement and Aims

At St John Henry Newman Catholic Primary School, we believe that digital technology and the internet are essential for learning, communication and creativity. However, we recognise the risks that children, staff, and the wider community may face online. This policy sets out our approach to keeping everyone safe online, promoting responsible digital behaviour, and ensuring compliance with statutory safeguarding requirements.

Aims:

- Protect pupils, staff, and the wider school community from online harm.
- Promote safe and responsible use of technology.
- Ensure compliance with safeguarding legislation and data protection.
- Provide clear guidance on roles, responsibilities and acceptable behaviour online.
- - Teach pupils to be digitally resilient and responsible citizens.

Section 2 – Scope

This policy applies to all staff, pupils, governors, volunteers, contractors and parents/carers who use the school's IT systems, devices, networks, or platforms, including personal devices used for school purposes. It covers internet, email, learning platforms, social media (in a school context), mobile devices, video conferencing and any online tools connected to school activity.

Section 3 – Principles and Legal Obligations

The school will:

- Safeguard children in line with Keeping Children Safe in Education and related statutory guidance.
- Ensure filtering, monitoring and network security are in place.
- Respect data protection requirements (UK GDPR, Data Protection Act 2018). - Promote responsible use of digital technology.

Section 4 – Roles and Responsibilities

Role	Responsibility
Governing Body	Approve and review policy; allocate resources; monitor implementation.
Headteacher	Overall responsibility for online safety; ensures training and response to incidents.
Designated Safeguarding Lead (DSL)	Point of contact for online safety; investigates concerns; liaises with agencies.
IT/Network Manager	Maintain filtering, monitoring, and security systems; support staff with technology safety.
Staff	Model safe behaviour; teach pupils online safety; follow procedures; report concerns.
Pupils	Use technology responsibly; follow rules; report concerns to staff.
Parents/Carers	Support safe online behaviour at home; reinforce school guidance; raise concerns if necessary.

Section 5 – Acceptable Use and Behaviour

- Staff use school-provided accounts and devices for school purposes.
- Pupils follow age-appropriate rules for online behaviour.
- No user should attempt to bypass filtering or monitoring systems.
- All communications must be respectful, lawful and considerate.
- Staff must model positive online behaviour, including use of social media (see Social Media Policy also).

Section 6 – Education and Training

- Pupils receive age-appropriate online safety education in curriculum and assemblies.
- Staff receive regular safeguarding and online safety training, including updates on emerging technologies and online risks.
- Parents/carers are supported with workshops, resources, and updates.

Online safety is taught through two complementary programmes:

- Ten Ten Life to the Full, the Diocese of East Anglia approved PSHE scheme.
- Project Evolve, which delivers age-appropriate learning mapped to the UK Council for Internet Safety Education Framework.

Teaching is progressive across all year groups and includes opportunities to revisit emerging online risks.

Pupils are taught to:

- recognise online abuse, grooming and exploitation;
- identify and report cyberbullying;
- critically evaluate information online, including misinformation and disinformation;
- understand the risks associated with social media, gaming and live streaming;
- recognise harmful online content, including content relating to violence, extremism, self-harm, suicide, eating disorders and inappropriate sexual content;
- understand the legal and safeguarding implications of creating, possessing or sharing nude or semi-nude images;
- recognise manipulated media, including deepfakes and AI-generated content, and understand that not everything seen online is genuine;
- understand the benefits and risks associated with generative artificial intelligence, including protecting personal information and avoiding over-reliance on AI-generated content.
-

Section 7 – Risk Assessment, Filtering and Monitoring

- Filtering systems block harmful and illegal content.
- Monitoring systems detect misuse; logs are reviewed by the Headteacher.
- Risk assessments cover online hazards (e.g., cyberbullying, grooming, data misuse).
- Filtering systems block access to harmful and illegal content in accordance with DfE filtering standards.
- Monitoring systems help identify concerning online behaviour and potential safeguarding risks.

Risk assessments consider emerging online risks, including:

- online abuse and exploitation;
- cyberbullying;
- exposure to harmful online content;
- misinformation and disinformation;
- sharing of nude and semi-nude images;
- misuse of generative AI, including deepfakes and manipulated imagery.

Staff remain professionally curious where online behaviour may indicate wider safeguarding concerns. Reports of harmful online activity are investigated promptly and proportionately.

Section 8 – Responding to Incidents

Responding to Online Safety Incidents

- Any member of staff who becomes aware of an online safety concern must:
    - ensure the child is safe;
    - avoid investigating beyond what is necessary to establish the immediate facts;
    - preserve any available evidence where appropriate;
    - report the concern immediately to the Designated Safeguarding Lead (DSL) or Deputy DSL.
- All online safety concerns must be recorded on **CPOMS** at the earliest opportunity.
- Where immediate advice is required, staff should speak directly to the DSL or DDSL before completing the CPOMS record.

The DSL will:

- assess the level of risk;
- consider whether the incident forms part of a wider safeguarding concern;
- liaise with parents/carers where appropriate;
- work with external agencies, including Children's Social Care, the Police or CEOP where necessary;
- ensure appropriate support is provided to any victim and educational intervention is provided for any child displaying harmful behaviour.

Specific procedures include:

Online abuse and exploitation

- Concerns regarding grooming, coercion, sexual exploitation or criminal exploitation online will be managed in accordance with the school's Child Protection and Safeguarding Policy.

Cyberbullying

- Reports of cyberbullying will be investigated promptly.
- Appropriate sanctions, restorative work and support will be implemented alongside safeguarding procedures where required.

Harmful online content

- Exposure to harmful, illegal or age-inappropriate material will be treated as a safeguarding concern.
- The DSL will assess whether additional support or referrals are required.

Misinformation and disinformation

- Staff will support pupils in critically evaluating online information.
- Deliberate sharing of harmful misinformation will be addressed through education and where appropriate, behaviour procedures.

Making, possessing or sharing nudes and semi-nudes

- The school will follow the Department for Education guidance **Sharing nudes and semi-nudes: advice for education settings working with children and young people**.
- Staff must never view, copy, print, share or forward indecent images unless there is no other reasonable option to safeguard a child.

- Any incident will be referred immediately to the DSL who will undertake an appropriate risk assessment and determine next steps.

Generative AI, deepfakes and manipulated imagery

- Any misuse of AI-generated content that places a child at risk, causes harm or damages another person's reputation will be managed as a safeguarding concern.
- Pupils will be supported to understand how AI-generated images, audio and video can be manipulated to deceive others.
- Allegations involving AI-generated or manipulated sexual images will be treated with the same seriousness as any other safeguarding concern.

Section 9 – Policy Review

This policy will be reviewed annually, or sooner if legislation, technology, or incidents require updates. Governors, staff, parents and pupils may be consulted during the review process.

Signatures

___ Headteacher: _____ Date: _____

___ Chair of Governors: _____ Date: _____