



Notre Dame High School

Sharing the love and goodness of God with everyone

Online Safety Policy 2026-2027

Policy Name	Online Safety Policy
Status	Live
Policy Author	Mr S. Scriven (Assistant Head)
Date Adopted	September 2026
Review Period	12 months
Last Review Date	September 2026
Next Review Date	September 2027
Approved by	Local Academy Committee

Contents

1. Introduction
2. Purpose and Scope Policy
3. Legal Framework
4. Our Commitment
5. Online Safety Education
6. Online Safety Curriculum
7. Understanding Online Risk
8. Curriculum Overview
9. Artificial Intelligence and Emerging Technology
10. Misinformation, Disinformation and Critical Thinking
11. Safeguarding Through Education
12. Roles and Responsibilities
13. Filtering and Monitoring
14. Sophos Filtering and Fastvue Monitoring
15. Reviewing Monitoring Reports
16. Understanding Fastvue Data
17. Cyber Security
18. Acceptable Use

1. Introduction

1.1 Institutional Commitment

Notre Dame High School is committed to creating a safe, respectful and inclusive digital environment in which every member of the school community can learn, communicate and flourish.

1.2 Educational Context

Digital technologies are central to education and everyday life. They provide significant opportunities for learning, creativity, communication and personal development. However, they also present safeguarding risks which require careful management through education, effective safeguarding procedures and robust technical systems.

1.3 Safeguarding Integration

Online safety is recognised as an essential element of safeguarding and child protection. It is not viewed as a stand-alone issue but is embedded throughout the school's safeguarding culture, curriculum, pastoral support and leadership.

1.4 Catholic Ethos and Mission

As a Catholic school, we believe every person is created in the image of God and deserves dignity, respect and protection. We therefore expect all members of our community to demonstrate kindness, integrity and responsibility in their online interactions, reflecting our Gospel values both within and beyond school.

2. Purpose and Scope of Policy

2.1 Policy Objectives

The purpose of this policy is to:

- Safeguard children and young people when using digital technologies.
- Promote safe, responsible and respectful use of online services.
- Support pupils in becoming confident and resilient digital citizens.
- Ensure appropriate filtering and monitoring arrangements are in place.
- Establish clear procedures for responding to online safeguarding concerns.
- Define the responsibilities of governors, leaders, staff, pupils and parents.
- Ensure compliance with statutory safeguarding guidance and current legislation.

2.2 Policy Scope

This policy applies to:

- All pupils.
- All members of staff.
- Governors.
- Volunteers.
- Contractors working on behalf of the school.
- Visitors using school digital systems.
- Anyone accessing school networks, devices or online services.

3. Legal Framework

3.1 Statutory Guidance and Legislation

This policy must be read alongside current legislation and statutory guidance including, but not limited to:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- The Children Act 1989 and 2004
- The Education Act 2002
- The Online Safety Act
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Equality Act 2010
- Prevent Duty Guidance
- Relationships Education, Relationships and Sex Education and Health Education statutory guidance
- DfE Filtering and Monitoring Standards for Schools and Colleges
- Searching, Screening and Confiscation Guidance
- Teaching Online Safety in Schools Guidance

3.2 Policy Review Trigger

The school will review this policy whenever statutory guidance changes or where local safeguarding arrangements require amendment.

4. Our Commitment

4.1 Core Principles

Notre Dame High School operates under the following guiding principles:

- o Every child has the right to feel safe online.
- o Safeguarding extends beyond the physical school environment into digital spaces.
- o Pupils should be empowered to enjoy technology safely rather than discouraged from using it.
- o Online safety is everyone's responsibility.
- o Education is the most effective long-term safeguard against online harm.
- o Parents and carers are essential partners in promoting safe online behaviour.

4.2 Proactive Adaptability

We recognise that online harms continue to evolve rapidly. Consequently, our curriculum and safeguarding procedures are reviewed regularly to ensure they reflect emerging technologies, current safeguarding concerns and national guidance.

5. Online Safety Education

5.1 Delivery Philosophy

Online safety education is a fundamental part of the school's safeguarding curriculum. Pupils are taught to use technology safely, respectfully, responsibly and critically throughout their time at Notre Dame High School. Learning is progressive, age-appropriate and responsive to emerging safeguarding risks.

5.2 Provision Channels

Online safety education is delivered through:

- o Relationships, Sex and Health Education (RSHE).
- o Life Skills.
- o Careers Education.
- o Computing curriculum.
- o School assemblies and tutor time.
- o Enrichment activities and Safer Internet Day initiatives.
- o External specialist speakers where appropriate.
- o Targeted pastoral interventions.

5.3 Emerging Threat Response

Where new online risks emerge, additional learning opportunities are provided dynamically through the tutor programme and safeguarding updates.

6. Online Safety Curriculum

6.1 Core Competencies

Our curriculum equips pupils with the knowledge, understanding and skills to:

- Protect their personal information online.
- Understand digital footprints and online reputation.
- Create and manage secure passwords.
- Recognise grooming, exploitation and coercive behaviour.
- Identify scams, fraud and financial exploitation.
- Understand healthy online relationships.
- Recognise and report cyberbullying.
- Seek help when concerned about online activity.
- Evaluate the reliability of online information.
- Recognise misinformation, disinformation and conspiracy theories.
- Understand the opportunities and limitations of Artificial Intelligence.
- Behave respectfully and lawfully online.
- Understand consent when sharing images or information.
- Know how to report concerns both within school and externally.

7. Understanding Online Risk

7.1 Department for Education (DfE) Risk Categories

The school actively teaches pupils about the four primary categories of online risk identified by the Department for Education:

Content Risks

Pupils learn to recognise and respond to harmful or inappropriate material, including:

- Pornography.
- Violent or disturbing content.
- Extremist material and hate speech.
- Self-harm content.
- Misinformation, disinformation, manipulated media and deepfakes.

Contact Risks

Pupils learn about threats associated with online communication, including:

- Grooming (sexual and criminal exploitation).
- Radicalisation and coercion.
- Unsafe online relationships with strangers.

Conduct Risks

Pupils develop an explicit understanding of responsible online behaviour, including:

- Respectful peer-to-peer communication.
- The prevention of cyberbullying.
- Consent and legal responsibilities regarding image sharing.
- Managing privacy settings and digital reputation.

Commerce Risks

Pupils are taught how to recognise commercial threats, including:

- Scams, phishing attempts and identity theft.
- Online gambling and predatory advertising.
- The risks of hidden in-app purchases and financial exploitation.

8. Curriculum Overview

The following multi-layered curriculum framework forms our formal online safety provision:

Year Group	Curriculum Content
Year 7 RSHE	<i>My Life on Screen</i> – Digital footprints, privacy, online relationships, cyberbullying, reporting concerns and safe online behaviour.
Year 8 RSHE	<i>Think Before You Share</i> – Digital reputation, image sharing, respectful communication, online consent, personal information and social media.
Year 9 RSHE	<i>Love People, Use Things & Understanding Consent</i> – Healthy online relationships, coercion, image sharing, consent, exploitation and online conduct.
Year 10 Life Skills	<i>Protecting Personal Data</i> – Privacy, scams, identity theft, passwords, financial security, digital resilience and personal information.
Careers Education	<i>Artificial Intelligence</i> – Future employment considerations, digital literacy and the responsible use of emerging technologies.
Whole School	Multi-channel delivery via assemblies, the tutor programme, Safer Internet Day, targeted enrichment activities and tactical safeguarding updates.

9. Artificial Intelligence and Emerging Technology

9.1 Educational Integration

The school recognises that Artificial Intelligence (AI) is rapidly transforming education and wider society. Pupils are actively taught to navigate both the immense opportunities and specific safeguarding risks associated with AI technologies.

9.2 Instructional Framework

Teaching regarding emerging technologies strictly includes:

- The responsible use of generative AI tools.
- Protecting personal data and privacy within AI interfaces.
- Recognising inaccurate, biased or hallucinated AI-generated content.
- Identifying deepfakes and synthetic media.
- Academic honesty, plagiarism prevention and intellectual property rights.
- The ethical implications of AI use in education and future employment.

9.3 Future Strategy

As national regulatory frameworks and Department for Education guidance develop, the school will continually review and adapt its digital strategy to ensure pupils remain secure and digitally literate.

10. Misinformation, Disinformation and Critical Thinking

Notre Dame High School recognises the increasing risks posed by misinformation, disinformation and conspiracy theories.

Pupils are taught to:

- question the reliability of online information;
- identify trustworthy sources;
- recognise manipulation through algorithms and social media;
- understand how false information spreads online;
- evaluate evidence critically before sharing information;
- recognise emotionally manipulative online content.

As revised national RSHE guidance is implemented, this area of learning will continue to expand across the curriculum.

11. Safeguarding Through Education

Online safety education is reviewed annually by the Designated Safeguarding Lead, curriculum leaders and senior leaders.

Curriculum planning is informed by:

- safeguarding data;
- local and national safeguarding priorities;
- pupil voice;
- parental feedback;
- emerging technologies;
- Ofsted expectations;
- statutory guidance;
- local safeguarding partnerships.

The school remains committed to ensuring that online safety education reflects current risks and equips pupils with the knowledge, skills and confidence needed to participate safely in an increasingly digital world.

12. Roles and Responsibilities

Safeguarding is everyone's responsibility. All members of the school community have a role to play in promoting safe and responsible use of technology.

Governing Body

The Governing Body has strategic responsibility for online safety and will:

- ensure the school meets its statutory safeguarding duties in relation to online safety;
- ensure appropriate filtering and monitoring systems are in place and reviewed regularly in accordance with Department for Education (DfE) guidance;
- receive regular safeguarding reports, including information relating to online safety incidents and emerging risks;
- ensure sufficient resources are available to maintain effective safeguarding arrangements;

- review this policy annually;
- ensure staff receive appropriate safeguarding and online safety training.

The Governing Body will seek assurance that filtering and monitoring arrangements remain effective and proportionate to the needs of the school.

Headteacher

The Headteacher is responsible for ensuring:

- this policy is implemented consistently across the school;
- online safety is embedded within the school's safeguarding culture;
- appropriate staffing and resources are available;
- staff receive regular safeguarding updates;
- pupils receive a progressive online safety curriculum;
- safeguarding concerns are managed effectively.

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead has operational responsibility for online safeguarding.

The DSL will:

- lead on all online safety matters;
- oversee filtering and monitoring systems;
- review safeguarding alerts and determine appropriate action;
- maintain accurate safeguarding records on CPOMS;
- provide advice and support to staff;
- liaise with parents, carers and external agencies where appropriate;
- monitor safeguarding trends to identify emerging risks;
- ensure online safety education remains current and effective;
- deliver safeguarding updates and staff training;
- report regularly to the Senior Leadership Team and Governors.

Deputy Designated Safeguarding Leads

Deputy DSLs will:

- support the DSL in managing safeguarding concerns;
- respond to safeguarding alerts in the absence of the DSL;
- contribute to safeguarding investigations;
- ensure concerns are appropriately recorded and followed up.

IT Network Manager

The Network Manager plays a key role in maintaining secure digital systems.

Responsibilities include:

- maintaining filtering and monitoring systems;

- ensuring appropriate security updates are applied;
- managing user accounts and permissions;
- supporting investigations into online incidents where required;
- advising senior leaders regarding cyber security risks;
- maintaining secure backups and network resilience;
- supporting compliance with DfE Filtering and Monitoring Standards.

The Network Manager does not make safeguarding decisions but works closely with the DSL where safeguarding concerns arise.

All Staff

Every member of staff has a responsibility to safeguard children online.

Staff will:

- model safe and professional online behaviour;
- follow the Staff Code of Conduct;
- report any online safety concerns immediately to the DSL;
- challenge inappropriate behaviour where appropriate;
- deliver online safety messages through the curriculum where relevant;
- undertake mandatory safeguarding and online safety training;
- remain vigilant to emerging safeguarding risks.

Staff should never assume that another colleague has reported a safeguarding concern.

Pupils

Pupils are expected to:

- use technology safely and responsibly;
- follow the school's Acceptable Use Agreement;
- treat others with kindness and respect online;
- protect their personal information;
- report any concerns to a trusted adult;
- use school equipment appropriately;
- respect copyright and intellectual property.

Pupils are encouraged to report concerns without fear of blame.

Parents and Carers

Parents and carers play a vital role in supporting online safety.

The school will encourage parents and carers to:

- discuss online safety regularly at home;
- monitor age-appropriate online activity;
- support responsible use of devices;
- reinforce the school's expectations regarding respectful online behaviour;

- report concerns to school promptly;
- attend online safety workshops where available.

The school will provide advice and guidance to parents as new online risks emerge.

13. Filtering and Monitoring

Notre Dame High School recognises that filtering and monitoring form an essential part of an effective safeguarding culture.

The school maintains filtering and monitoring arrangements that are appropriate to the age of pupils, the school's safeguarding risk assessment and current statutory guidance.

Filtering and monitoring systems are not intended to replace professional curiosity or staff vigilance but provide an additional safeguard for children and young people.

Filtering and monitoring arrangements are reviewed:

- annually;
- following significant changes to technology;
- following safeguarding incidents;
- where new safeguarding risks emerge;
- following updates to DfE guidance.

Filtering

The school's filtering systems are designed to:

- prevent access to illegal material;
- reduce exposure to harmful online content;
- support teaching and learning;
- minimise safeguarding risks;
- comply with statutory guidance.

The school balances appropriate safeguarding with educational access to legitimate online resources.

Monitoring

Monitoring systems are used to identify safeguarding concerns including, but not limited to:

- self-harm;
- suicidal ideation;
- child sexual abuse material;
- extremism and radicalisation;
- bullying;
- online abuse;
- harmful sexual behaviour;
- inappropriate language;
- safeguarding disclosures;
- attempts to bypass filtering systems.

Monitoring is proportionate, risk-based and undertaken for safeguarding purposes only.

14.Sophos Filtering and Fastvue Monitoring

Notre Dame High School uses Sophos filtering together with Fastvue reporting and monitoring software to provide real-time safeguarding alerts across the school's digital infrastructure.

These systems assist the safeguarding team by identifying activity that may indicate a safeguarding concern. Monitoring is undertaken in accordance with UK GDPR, safeguarding legislation and the school's Data Protection policies.

Real-Time Safeguarding Alerts

Where the monitoring system identifies activity that may indicate a safeguarding concern, alerts are automatically generated for the Designated Safeguarding Lead.

Depending upon the level of risk, responses may include:

Online Safety Concerns

Where concerns relate to inappropriate searches, websites or online behaviour, the DSL may:

- investigate the circumstances;
- speak with the pupil;
- liaise with pastoral staff;
- record the concern on CPOMS;
- contact parents or carers where appropriate.

Self-Harm or Suicide Risk

Alerts indicating possible self-harm or suicidal ideation are treated as a safeguarding priority.

The DSL or Deputy DSL will:

- assess the concern immediately;
- speak with the pupil where appropriate;
- inform parents or carers as soon as possible;
- record actions on CPOMS;
- involve external agencies where necessary.

Radicalisation

Where monitoring identifies activity suggesting possible radicalisation or extremist content, the school will respond in accordance with its Prevent Duty procedures.

This may include:

- discussion with the pupil;
- safeguarding assessment;
- contact with parents or carers;
- referral to external safeguarding partners where appropriate.

Other Safeguarding Concerns

Where monitoring identifies concerns relating to exploitation, abuse or criminal activity, the DSL will determine the most appropriate safeguarding response, including referral to Children's Social Care, the Police or other relevant agencies where necessary.

15. Reviewing Monitoring Reports

In addition to real-time alerts, the DSL reviews routine monitoring reports to:

- identify patterns of behaviour;
- monitor emerging safeguarding risks;
- evaluate the effectiveness of filtering systems;
- inform safeguarding risk assessments;
- identify curriculum needs;
- improve preventative education.

Where repeated concerns are identified, appropriate intervention and support will be provided.

16. Understanding Fastvue Data

The school recognises that automated monitoring systems may occasionally generate alerts where no inappropriate content has actually been viewed.

Where Fastvue reports indicate a data transfer of less than **1000 bytes (1KB)**, this will normally indicate that:

- a website has been successfully blocked before content loaded;
- only a blocking page was displayed;
- the connection was terminated before any meaningful content was accessed;
- advertising or background scripts triggered an alert without user intent.

Such alerts will normally require no further safeguarding action, however, professional judgement will always be exercised.

Where repeated attempts are made to access blocked content, even where individual alerts involve minimal data transfer, the DSL may investigate further to determine whether there is evidence of deliberate attempts to circumvent school filtering systems.

Safeguarding decisions will always be based upon the wider context rather than automated alerts alone.

17. Cyber Security

The school is committed to maintaining secure digital systems.

Appropriate measures include:

- secure passwords and authentication;
- role-based access permissions;
- encrypted devices where appropriate;
- regular software updates;
- antivirus protection;
- secure backup procedures;
- cyber security awareness training;
- incident response procedures.

Any suspected cyber security breach will be reported immediately to senior leaders and managed in accordance with the school's Data Protection and Cyber Security procedures.

18. Acceptable Use

All users of the school's digital systems are expected to use technology responsibly.

Separate Acceptable Use Agreements are provided for:

- pupils;
- staff;
- governors where appropriate.

Failure to comply with these agreements may result in disciplinary action and, where appropriate, safeguarding intervention.

The school reserves the right to restrict or remove access to school systems where misuse places individuals or the wider community at risk