



**Our Lady and All Saints**  
Catholic Multi Academy Company  
Strong in Faith

# Online Safety Policy

As a Catholic Multi Academy Company, we exist to secure, protect and enrich Catholic Education across our family of schools. We seek to ensure that the future Catholic education is secure and stable through effective governance and parish engagement and to develop curriculum and standards that reflect the Catholic Life approach and ethos.

<b>Ratified by:</b>	Peter Davis, CEO
<b>Date ratified:</b>	17 <sup>th</sup> October 2025
<b>Name of originator/author:</b>	Chief Information Officer
<b>Date issued:</b>	20 <sup>th</sup> October 2025
<b>Review date:</b>	October 2026

## 1. Introduction

This policy supports the school's duty to safeguard all pupils and staff when using technology.

It reflects the requirements of *Keeping Children Safe in Education (2025)* and the *Department for Education Cyber Security Standards*, ensuring that online safety, cyber security and data protection are fully embedded in our safeguarding practice.

The policy has been developed under the direction of the OLAAS Chief Information Officer to provide a consistent approach across all OLAAS schools until the full MAC-wide digital safeguarding policy is approved.

Local information such as the Designated Safeguarding Lead (DSL), Online Safety Governor and review dates should be added by each school.

## 2. Scope

This policy applies to everyone who uses the school's digital systems, including staff, pupils, governors, volunteers, visitors and contractors.

It covers the use of all digital technology in school and remotely, including the internet, e-mail, mobile devices, cloud platforms, and any AI-based systems used by staff for teaching, learning or administration.

## 3. Aims

The aims of this policy are to:

- Protect pupils and staff from risks associated with the use of technology.
- Promote safe, respectful and responsible behaviour online.
- Embed digital safeguarding and cyber awareness within the wider safeguarding framework.
- Clarify staff responsibilities for the appropriate use of digital and AI tools.

## 4. Roles and Responsibilities

### Headteacher and Senior Leaders

- Hold overall responsibility for online safety within the school.
- Ensure this policy is implemented and reviewed each year.
- Work with the DSL, Online Safety Lead and IT provider to monitor filtering, monitoring and cyber-security arrangements.

### Designated Safeguarding Lead (DSL)

- Leads on online safety and digital safeguarding.
- Ensures all staff understand current risks and how to report concerns.
- Oversees filtering, monitoring and any incidents involving digital systems or AI.
- Provides and records annual training for staff on online safety and cyber awareness.

### IT Lead / Service Provider

- Maintains secure systems that meet DfE Cyber Security Standards.
- Reviews filtering and monitoring logs with the DSL.
- Ensures regular backups, encryption and secure disposal of old equipment.

### All Staff

- Follow this policy and the school's Acceptable Use Agreement.
- Use only approved systems and applications.
- Exercise professional judgement and report any concerns immediately to the DSL.

## 5. Cyber Security

Cyber security protects school data and systems from loss, misuse or harm. It is part of safeguarding.

The school will:

- Complete an annual cyber-risk assessment.
- Use multi-factor authentication (MFA) where appropriate.
- Test backup and restoration procedures regularly.
- Securely wipe or dispose of redundant devices.
- Record and report any cyber incident or data breach to the DSL and DPO, and to the ICO where required.

## 6. Artificial Intelligence (AI)

AI and other emerging technologies can be valuable tools for staff when used appropriately. For primary pupils, the focus is on understanding AI, not using it directly.

- Only staff may access AI systems for approved educational or administrative tasks.
- Pupils learn about AI through age-appropriate discussions and lessons on digital literacy.
- AI must support, not replace, professional judgement or teaching practice.
- Staff remain responsible for all content produced or adapted with AI.
- Personal or identifiable pupil data must never be entered into AI systems.
- Any concern about AI misuse or unsuitable material must be reported to the DSL.

## 7. Filtering, Monitoring and Data Protection

- Filtering and monitoring systems are reviewed at least annually and after any significant change.
- The DSL, IT provider and responsible governor review the outcomes together.
- Records of reviews and incidents are kept and reported to governors.
- All personal data is managed in line with **UK GDPR** and the school's **Data Protection Policy**.

## 8. Training and Awareness

- All staff receive annual safeguarding training that includes online safety, cyber security and data protection.
- Staff are being introduced to the principles of responsible and ethical AI use as this develops across the MAC.
- Pupils are taught about online safety, digital wellbeing and respectful behaviour online through the curriculum and assemblies.

## 9. Governance and Review

- The Safeguarding Governor meets termly with the DSL.
- Governors receive an annual report on online safety, filtering, monitoring, cyber security and AI.
- This policy is reviewed each year or earlier if there are significant changes in guidance or technology.

## 10. Interim Statement

This policy is issued as an interim version for OLAAS Catholic MAC schools. It ensures a consistent approach to digital safeguarding, online safety and cyber security until the final MAC-wide Online Safety and AI Policy is adopted.