Holy Cross

CATHOLIC HIGH SCHOOL

Internet Access Policy

'I have come that they may have life, and have it to the full' (John 10:10).

Owner: Headteacher / Designated Safeguarding Lead (DSL) & IT Strategic Lead
Approved by: Governing Body Autumn 2025
Review cycle: Annual or following significant change in guidance/technology
Next scheduled review: Autumn 2026

1. Purpose & Scope

This policy sets out how the school provides safe, secure and responsible access to the internet, email, cloud services and digital devices. It applies to all pupils, staff, governors, contractors and visitors using school-managed or personal devices to access school networks, systems or data.

2. Legal & Policy Framework

This policy aligns with current UK statutory and advisory guidance, including:

- Keeping Children Safe in Education (KCSIE) 2025 (DfE)
- DfE Digital & Technology Standards: Filtering and Monitoring; Cyber Security (2022 Updated 2025)
- Prevent Duty Guidance for England and Wales (Home Office, 2023, updated 2024)
- UK GDPR and Data Protection Act 2018; ICO guidance on education data and the Children's Code
- National cyber security center guidance on passwords, multi-factor authentication (MFA) and cyber security in schools
- Computer Misuse Act 1990
- Internet Watch Foundation (IWF) reporting guidance.

3. Roles & Responsibilities

Governing Body: Approves this policy; ensures resources and oversight for filtering, monitoring and cyber security.
Headteacher: Ensures implementation; allocates responsibilities; ensures suitable training, monitoring and incident management.
Designated Safeguarding Lead (DSL): Leads online safety, including risk assessment, curriculum, response to concerns and liaison with external agencies.
Strategic Lead for Whole School ICT: Implements technical controls (filtering, monitoring, backups, patching, MFA); maintains audit logs; conducts regular reviews.
Data Protection Officer (DPO): Advises on UK GDPR compliance, DPIAs and data handling; supports incident response and breach reporting.
Staff: Model safe and responsible use; follow this policy; complete required training on an annual basis; report concerns or incidents immediately to the IT Strategic Lead.
Pupils/Students: Use technology responsibly for learning; follow the Pupil Acceptable Usage Policy; report anything that makes them uncomfortable or unsafe to a member of staff.
Parents/Carers: Support the school's approach to online safety; discuss online behaviour with their child; sign the Parent/Carer home school agreement acknowledgment.

4. Access, Accounts & Authentication

- Named user accounts are issued for staff and pupils; sharing credentials is prohibited.
- Strong authentication is required for staff and any account with access to sensitive data or admin functions; MFA is mandatory where supported (app-based preferred).
- Default passwords are changed on first use and never reused across systems.
- Access follows the principle of least privilege and is removed promptly when no longer required.

5. Web Filtering & Monitoring

The school operates age-appropriate filtering and proportionate monitoring on all school-managed networks and devices. Provision is reviewed at least annually and after incidents or significant changes. Over-blocking is avoided to enable effective teaching and learning.

- Roles and responsibilities for managing filtering and monitoring are defined and reviewed annually.
- Filtering blocks illegal, inappropriate and harmful content; categories and exceptions are documented and approved.
- Monitoring strategies (technical and supervisory) are risk-based and focus on safeguarding while respecting privacy.
- Alerts and reports are reviewed promptly by trained staff with clear escalation to DSL and senior leaders.

6. Education for Online Safety & Digital Citizenship

Online safety is taught across a range of subject disciplines including through PSHE/RSE. Teaching includes critical evaluation of online information, privacy and security, respectful behaviour, and managing online wellbeing.

7. Email, Messaging & Collaboration Tools

- School-provided accounts (eg Microsoft 365) must be used for school business; personal accounts must not be used for school-related activities and pupil data.
- Phishing awareness is mandatory; suspicious messages must be reported to IT.
- Auto-forwarding to personal accounts is disabled for staff by default.
- Professional standards of communication apply to all messages and posts.

8. Data Protection & Privacy

- Personal data is processed lawfully, fairly and transparently under UK GDPR and the Data Protection Act 2018.
- A DPIA is completed for high-risk processing (eg new platforms, biometric systems, online proctoring).
- Data is encrypted in transit and at rest where appropriate; secure configurations are enforced on managed devices.
- Only approved cloud services under appropriate contracts and data processing agreements may be used.
- Subject Access Requests are handled in line with ICO guidance; retention and deletion follow the school's Records Management Schedule.

9. Mobile Devices & Bring Your Own Device

- Personal devices may connect to the guest networks only with permission.
- Devices must be locked with a passcode/biometric, kept updated and have security enabled; jail-broken/rooted devices are not permitted.
- Storing school personal data on unmanaged personal devices is prohibited unless specifically approved with controls in place this includes portable storage devices.

10. Generative Artificial Intelligence (AI) & Emerging Technologies

Use of AI tools (eg content generators, transcription, adaptive learning) must be transparent, ethical, and compliant with data protection. Staff must avoid entering personal or sensitive data into AI tools. Pupils may use AI to support learning when explicitly permitted by teachers; all submitted work must be the learner's own with AI support acknowledged. The school provides guidance on academic integrity and plagiarism. Staff and Pupils must adhere to and stay inline with the AI usage policy.

11. School Website, Social Media & Digital Publishing

- Only approved staff may publish content on official channels; content must be accurate, respectful, and protect pupils' identities as appropriate.
- Use of pupil images requires appropriate consent and risk assessment; geo-tagging and personal contact details are not published.
- The school's address and office contact details act as the public point of contact; staff's personal contact details are not published.

12. Behaviour, Anti-Bullying & Wellbeing (including outside school)

Bullying, harassment or discrimination online is unacceptable and will be addressed under the Behaviour and Anti-Bullying policies. Where conduct outside school impacts the welfare of pupils or staff, the school may take proportionate action in line with statutory guidance and local policies.

13. Incident Reporting & Response

- All users must report safeguarding concerns, suspected cyber incidents, data breaches or exposure to illegal content immediately to the DSL or Deputy DSL/IT Strategic Lead.
- The school will preserve evidence, contain the issue, and notify stakeholders as required (including ICO within 72 hours where a notifiable personal data breach occurs).
- Illegal content (eg child sexual abuse material) will be reported to the Internet Watch Foundation (IWF) and, if necessary, the police. Terrorist content will be reported via the Action counter terrorism (ACT) process and Prevent.

14. Technical & Security Standards

- Apply vendor-supported security updates promptly on servers, endpoints and network devices.
- Maintain centrally managed anti-malware and DNS filtering; implement email security controls
- Use regular, tested offline/immutable backups for critical systems and data.
- Control admin privileges; use separate admin accounts and enforce MFA for privileged access.
- Log and review security events; retain logs per policy to support investigations.

Updated Autumn Term 2025
Review December 2026