Our Lady and All Saints Catholic Multi Academy Company

Secondary Online Safety Policy

Version:	1.0
Ratified by:	CSEL, Peter Davis
Date ratified:	24th March 2026
Name of originator/author:	Ben Clayton - October 2025
Issue Date:	7th April 2026
Review date:	October 2026

Interim MAC-Wide Version – Updated to include DUAA 2025 and 2025 DfE Filtering & Monitoring requirements

1. Policy Purpose

This MAC-wide policy sets the standards for online safety, digital safeguarding, cyber security, and responsible technology use across all OLAAS secondary schools. It ensures that schools:

- Comply with all statutory safeguarding requirements
- Follow DfE Digital & Cyber Security Standards
- Meet DfE Filtering & Monitoring Standards (2023, updated 2024/25 guidance)
- Protect student and staff data under UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025
- Manage risks related to online harms, mobile technology, social media, and AI
- Operate consistent systems across the MAC while allowing for local procedures

2. Scope

This policy applies to all members of the school community, including:

- Students
- Staff and volunteers
- Governors and trustees
- Contractors and service providers
- Visitors

It covers all digital and technological use, including:

- School-owned devices and networks
- Personal devices (BYOD) used on site
- Cloud platforms and online communication systems
- AI and automated decision-making systems
- Filtering, monitoring and cyber-security systems
- Remote access systems

3. Aims

- Safeguard all users online
- Prevent access to harmful or illegal content
- Promote responsible digital behaviour
- Clarify roles and responsibilities
- Ensure compliance with DUAA 2025, UK GDPR and DPA 2018
- Maintain secure digital systems aligned with DfE standards
- Ensure transparency and accountability in the use of technology

4. Key Categories of Online Risk (KCSIE 2025)

1. Content – harmful/inappropriate material
2. Contact – harmful interactions, grooming, exploitation
3. Conduct – harmful behaviour, bullying, image-sharing
4. Commerce – scams, phishing, gambling, fraud

5. Legislation and Guidance

Statutory

- Keeping Children Safe in Education (2025)
- Data (Use and Access) Act 2025
- UK GDPR / Data Protection Act 2018 (amended)
- Prevent Duty Guidance (2023)
- Education Act 2002
- Education and Inspections Act 2006
- Education Act 2011 (searching powers)
- Equality Act 2010
- Searching, Screening & Confiscation (2022)

DfE Digital & Cyber Standards

- DfE Filtering and Monitoring Standards (2023 + 2024/25 clarifications)

- DfE Cyber Security Standards (2023)

Additional Guidance

- Teaching Online Safety in Schools (DfE, 2019)
- UKCIS Sharing nudes & semi-nudes (2020)
- National Curriculum – Computing (2014) / RSHE (2020)

6. Roles and Responsibilities

6.1 MAC Chief Information Officer (CIO)

- Ensures MAC-wide compliance with filtering, monitoring and cyber standards
- Leads digital safeguarding strategy
- Oversees DUAA 2025 compliance related to digital systems
- Works with IT partners to maintain secure systems

6.2 Local Governing Body

- Approves this policy and acknowledges MAC-issued annexes
- Monitors compliance with digital standards
- Reviews annual online-safety report
- Ensures provision for vulnerable learners

6.3 Headteacher

- Ensures staff follow the policy
- Supports DSL and IT staff
- Implements DUAA and DfE standards
- Ensures appropriate training and oversight

6.4 Designated Safeguarding Lead (DSL)

- Leads online safety and digital safeguarding
- Reviews and escalates monitoring alerts
- Logs incidents in CPOMS
- Ensures staff training
- Completes filtering/monitoring risk assessment
- Ensures DPIAs for digital/AI systems (DUAA requirement)

6.5 IT Manager / IT Provider

- Maintains secure infrastructure
- Ensures compliance with DfE cyber standards
- Manages filtering and monitoring systems
- Maintains logs and records
- Reports security incidents to DSL, Headteacher and CIO

6.6 All Staff

- Follow this policy and Acceptable Use Agreements
- Report concerns immediately
- Use only approved systems
- Follow DUAA 2025 data handling rules

6.7 Students

- Follow Pupil AUA
- Report concerns promptly

7. Filtering & Monitoring (Updated for 2025)

All schools must meet DfE Filtering & Monitoring Standards (2023) and the strengthened 2024/25 expectations.

7.1 Roles & Responsibilities

Schools must record named individuals for:

- Senior Leader Responsible
- DSL
- IT Manager / Provider
- Online Safety Governor

7.2 Annual Review (Mandatory)

A documented annual review must be completed and signed off by:

- DSL
- Headteacher
- IT Manager / Provider
- Online Safety Governor
- MAC CIO

The review must include:

- Filtering/monitoring risk assessment
- Incident logs
- Evidence of system testing
- Review of AI, deepfake and emerging risks

7.3 Filtering Requirements

Filtering must:

- Block harmful/illegal content (IWF/CTIRU lists)
- Be age/role appropriate
- Balance safeguarding and learning (avoid overblocking)
- Apply to:

    - School devices on/off site
    - Cloud platforms
    - BYOD where required
    - Guest access
    - Mobile/hotspot access to school systems
- Record all filtering changes

7.4 Monitoring Requirements

Monitoring must:

- Include behavioural/contextual indicators
- Detect self-harm, extremism, sexual content, violence
- Include audit logs from Google/Microsoft platforms
- Trigger alerts reviewed daily by DSL/Deputy
- Maintain secure log retention
- Document all responses

7.5 Evidence for Ofsted/DfE

Schools must maintain evidence of:

- Annual reviews
- Logs and alerts
- Meeting minutes
- Filtering change records
- Training records

8. Cyber Security (DfE Standards)

Schools must:

- Use MFA for admin and privileged access
- Patch devices/systems regularly
- Test backups
- Use malware/ransomware protection
- Encrypt all school devices
- Maintain audit logs
- Securely dispose of IT equipment
- Report incidents to DSL → Headteacher → CIO

9. Artificial Intelligence & Automated Decisions (DUAA 2025)

Schools must ensure:

- No solely automated decision significantly affects a student
- Human oversight for AI-assisted processes
- Personal data is not entered into AI tools
- DPIAs for all AI or automated systems

- Students only use AI when approved and supervised
- AI misuse (deepfakes, cheating, harmful content) is treated as a safeguarding concern

10. Mobile Technology

Each school will insert its local phone procedures.

Minimum MAC expectations:

- No hotspotting to bypass filtering
- Clear rules for Bluetooth/AirDrop
- Clear rules for wearables and covert recording
- Mobile data risks addressed
- Sanctions for misuse

11. Digital Literacy & Curriculum

Schools must deliver online-safety learning via:

- RSHE / PSHE
- Computing
- Personal Development
- Assemblies and tutor time

Curriculum must include:

- Sexual harassment online
- Sexting/image-based abuse
- Extremism and radicalisation
- Hate content and misogyny
- Scams/fraud/phishing
- AI manipulation and deepfakes
- Mental health risks (self-harm, suicide, ED content)
- Digital resilience

12. Incident Reporting

All incidents must be:

1. Reported immediately to the DSL
2. Logged in CPOMS
3. Risk assessed and escalated
4. Reported to police where criminal content found
5. Reviewed for filtering/monitoring improvement

Searching devices must follow:

- DfE Searching & Screening Guidance
- UKCIS Nudes/Semi-nudes Guidance

13. Data Protection & DUAA 2025

Schools must:

- Provide enhanced protection for children's data
- Maintain data minimisation practices
- Complete DPIAs for new systems
- Ensure human oversight of any automated decision
- Follow DUAA SAR rules: clarification allowed; reasonable and proportionate search
- Comply with revised PECR requirements for cookies and e-communications

14. Training

Staff must receive annual training covering:

- Online risks
- DUAA 2025 changes
- Filtering & monitoring systems
- AI risks
- Cyber security
- Sexting and image-based abuse
- Digital safeguarding indicators

Governors and volunteers receive appropriate training.

15. Monitoring and Review

This policy is reviewed:

- Annually by DSL and CIO
- After significant incidents
- Following legislative changes
- Alongside Annex A (DUAA Compliance)

16. Annexes and Appendices

Annex A – Data (Use and Access) Act 2025 Compliance Addendum
(Updated by the CIO as legislation evolves.)

Appendices (school-specific):

- Acceptable Use Agreements
- Local Reporting Flowcharts
- Filtering & Monitoring Review Template
- SAR Handling Template
- AI Processing DPIA Template
- Local Mobile Phone Policy
- Incident Logging Guide

End of Policy

Appendix A – JHNCC Local Arrangements (Online Safety)

1. Parent/Carer Engagement (JHNCC)
JHNCC supports parents and carers to help children stay safe online through regular communication (for example: website guidance, newsletters and targeted sessions where appropriate). Parents and carers are encouraged to report any online safety concerns to the College, including incidents occurring outside College that impact pupils in College. Advice and signposting will be shared to support safe and responsible use of technology at home. This Online Safety Policy, including this appendix, is published on the College website.

2. Cyber-bullying (JHNCC)
Definition: Cyber-bullying is bullying behaviour carried out through technology (for example: messaging apps, social media, group chats, email, gaming platforms and image/video sharing). It may include harassment, intimidation, threats, exclusion, impersonation, sharing private information or images, or encouraging others to target someone.
Reporting and recording: Pupils and parents/carers should report concerns as soon as possible to a trusted adult, Head of Year/Pastoral Team, or the Designated Safeguarding Lead (DSL) where safeguarding may be involved. Staff must follow safeguarding procedures where a child may be at risk. Incidents will be recorded in line with College systems: behaviour incidents are logged on Class Charts in accordance with the Behaviour Policy, and safeguarding concerns are recorded via the College's safeguarding recording system, as appropriate.

Evidence: Where possible, preserve evidence (for example: screenshots, message links, usernames and timestamps). Pupils should be advised not to respond or retaliate.

Response: Cyber-bullying is treated as a serious behaviour matter. The College will respond in line with the Behaviour Policy (including proportionate sanctions and restorative approaches) and will provide support to pupils affected. Where appropriate, the College will also take steps to prevent recurrence and to protect pupils in College.

Off-site incidents: Where online behaviour occurs outside College but has an impact on pupils' safety, wellbeing or conduct in College, the College will respond in line with its policies. In line with national guidance, the College may apply sanctions where this is reasonable and lawful and where the pupil is identifiable as a pupil at the College, or the behaviour could have repercussions for the orderly running of the College, or it poses a threat to another pupil.

Escalation: Incidents involving threats, extortion, hate, coercive control, sexual content, image-based abuse or persistent targeted abuse may be treated as safeguarding and/or referred to external agencies (including the police) where appropriate.

3. Linked Policies (JHNCC)
This appendix should be read alongside: Behaviour Policy; Child Protection and Safeguarding Policy; Staff Code of Conduct/Staff Behaviour Policy; Acceptable Use Policies (Staff, Pupil and Visitor); Mobile Phone/Device Policy; RSHE/PSHE curriculum documentation; Complaints Policy; and the OLAAS Data Protection Policy.