OUR LADY & ST OSWALD'S
CATHOLIC PRIMARY SCHOOL

"I came so that they might have life and have it more abundantly."
John 10:10

Online Safety and Acceptable Use Policy

Academic year 2026 to 2027

Document control	Details
Status	Review draft for authorised approval — not yet in force
Version and reference	2.0 | OLSO-POL-ONLINE
Prepared and guidance checked	2 October 2026
Policy owner	Conor Meehan Headteacher with the DSL team and commissioned IT support
Accountability and approval	Our Lady Help of Christians Catholic Academy Trust; approval under the current Scheme of Delegation
Approval and effective date	To be recorded following authorised approval
Next planned review	September 2027 or sooner following material change

This policy sets out safe use of school technology, online safeguarding, teaching, communications and acceptable use. It applies to pupils, staff, governors, volunteers, contractors and others using school systems, including remote school activity. The safeguarding policy governs urgent protection and referral.

Our promises: We Are Kind • We Make Safe Choices • We Try Our Best

Core policy 1 of 2

Purpose and accountability

Pupils learn to use technology safely, critically and respectfully. This policy applies to pupils, staff, governors, volunteers and other users of school systems, including remote learning and off-site conduct affecting safety. Conor Meehan provides senior oversight with the DSL team; commissioned IT support operates technical controls. Safeguarding decisions remain with the school, not the filter or provider.

Teach and supervise

Teach age-appropriate online safety through the approved curriculum: content, contact, conduct and commerce, including bullying, grooming, scams, misinformation, privacy and AI-generated material. Explain how to report a mistake or concern without fear of automatic blame. Adapt teaching for age, SEND and communication needs. Do not bypass service age limits or require pupils to create unsuitable personal accounts. Supervision and purposeful teaching remain necessary when filtering is active.

Filtering and monitoring

Leaders and IT support review effectiveness at least once each academic year and after significant changes. Cover all school-connected devices and relevant locations; test controls, identify gaps and avoid unnecessary barriers to learning. Record the review, action owners and follow-up. Confirm the named human recipient, response arrangements and cover for monitoring alerts before systems are relied upon. Blocking content does not close a safeguarding concern. Staff report bypasses, unsuitable material or missed alerts promptly.

Accounts devices and communication

Use individual accounts, strong access controls and multi-factor authentication where available. Use approved storage, software and school communication channels; lock unattended devices and report security problems immediately. Do not share passwords, bypass controls with hotspots or use personal cloud storage for school records.

Pupil phones and ordinary smart devices follow Behaviour for Learning: switched off and handed in under the school arrangements throughout the school day, including breaks, with planned medical or disability exceptions. Apply agreed arrangements to school-run provision and visits. Staff keep personal phones away when working with pupils and use approved devices for school images, particularly in early years.

Core policy 2 of 2

Professional conduct images and AI

Use professional accounts and approved channels for contact with pupils and families. Do not conduct private social-media conversations with pupils. Follow the Staff Code of Conduct and the school's photography permissions, lawful basis and safeguarding restrictions; do not post pupil information or images through personal accounts.

Only use AI tools approved by school and Trust arrangements and appropriate to users' ages. Do not enter identifiable pupil, family or staff information into unapproved systems. Check factual accuracy, bias, suitability and copyright. AI does not make safeguarding, assessment, admission or disciplinary decisions on its own.

Respond to an incident

Protect the pupil, stop further exposure where safe and inform the DSL directly and promptly. Call 999 for immediate danger. Record safeguarding facts on CPOMS and notify IT support where technical action is needed; neither step replaces the other. Do not conduct an informal investigation or promise secrecy.

For sexual images of children, including synthetic or AI-generated images, do not routinely view, copy, print, forward or delete them. Do not ask the child to send an image. Secure the device, preserve relevant information safely and follow DSL and police directions. The DSL applies current UKCIS and KCSIE procedures.

Report adult conduct concerns to the Headteacher, or through the Chair/Trust route if the concern involves the Headteacher. Report suspected data breaches immediately under Confidentiality and Information Sharing; do not wait for the end of the day.

Agree use and work with families

Teach the pupil commitments in Appendix A and revisit them as understanding develops; an agreement is not a substitute for supervision. Adults read and follow the undertaking before accessing systems. Give families accessible information about learning platforms, reporting routes, device expectations and relevant risks. Respond to off-site harm affecting pupils through safeguarding and behaviour arrangements.

Required reference and review

Appendix A contains pupil and adult acceptable-use commitments. The Headteacher maintains a current technical contact and alert-cover record alongside the filtering review. Read with Safeguarding, Prevent, Behaviour for Learning, Confidentiality and Information Sharing, SEND and the Trust Staff Code of Conduct and data-protection policies. Review annually and after significant incidents, system or guidance changes.

Appendix A Acceptable use commitments

Required for pupils with age-appropriate adult explanation, and for every adult before using school systems.

Pupil acceptable use agreement

Nursery and younger pupils

- I use the device with the adult's help.
- I use the activities my adult has chosen.
- I am kind when I use technology.
- I stop and tell an adult if something worries me or appears by mistake.
- I ask before taking a picture or sharing something about another person.

Older primary pupils

- I use my own school account and keep my password private.
- I follow the task, use approved services and do not bypass school controls.
- I treat others kindly and do not make, request or share harmful or private images or messages.
- I keep personal information private and ask before sharing another person's information or image.
- I check what I read and know that online and AI content can be false or misleading.
- I report unsafe contact, unkind behaviour, a mistake or worrying material to a trusted adult promptly.
- I follow the school phone arrangements and ask an adult about any agreed exception.

An adult teaches these expectations in accessible language and checks understanding. The agreement supports teaching; a signature does not transfer responsibility for safeguarding to a child. Pupil/class: _____ Adult/date: _____

Adult acceptable use undertaking

I will use authorised accounts, devices and systems for the agreed purpose; maintain professional boundaries; secure credentials and information; follow image, monitoring and personal-device rules; report safeguarding/security concerns promptly; and comply with the Trust Staff Code of Conduct, data protection, social-media and acceptable-use provisions. I understand that authorised proportionate monitoring may occur and that lawful safeguarding/whistleblowing reports remain permitted.

Name and role: _____
Signature: _____
Date and induction/briefing: _____

Appendix B Sources and linked policies

Reference for the Headteacher, DSL and IT lead.

Linked policies and review

Read this policy alongside Child Protection and Safeguarding; Preventing Radicalisation; Behaviour for Learning and Behaviour Curriculum; SEND and Accessibility arrangements; Relationships and Health Education and Computing curriculum; Confidentiality and Information Sharing; Trust Data Protection, ICT Acceptable Use, Social Media, Staff Code of Conduct, Safer Recruitment and Whistleblowing procedures. The Trust framework governs employment, complaints and data protection. This policy sets out the school's local implementation; it does not alter the Trust's legal accountability or statutory rights.

The owner checks actual arrangements and staff competence before issue. The authorised approving body records the approval and effective date; staff are briefed and parents receive accessible information where relevant. Review annually and earlier following a significant incident, changed needs, personnel, provision or guidance. Companion review drafts retain their own approval status. Urgent protective action does not wait for policy approval.

Source register

Public sources checked on 2 October 2026. Statutory guidance, non-statutory advice and school choices have different status. Publication-page links allow later editions to be checked. Local arrangements derive from the supplied policies and the Headteacher's school context; the accompanying audit identifies facts requiring confirmation.

Keeping children safe in education 2026

DfE statutory guidance in force from 1 September 2026

Information Sharing Duty

DfE statutory guidance September 2026 and Children Act 2004 section 16LA duty in force from 30 September 2026

The Prevent duty practical guidance for designated safeguarding leads

DfE operational guidance updated 24 September 2026

Early years foundation stage statutory framework

Group and school-based providers version in force from 1 September 2026

Trust sources: OLHOC Personnel Policies 2025–26 and Statutory Policy Handbook 2025–26, supplied September 2025 editions with September 2026 review dates. Confirm the current editions and Scheme of Delegation. School sources include Our Vision, Values and Aims 2.0, Behaviour for Learning, Attendance and Punctuality, SEND and ASP arrangements, and the recent Mathematics, Uniform, Accessibility and SEMH drafts where relevant.