ONLINE SAFETY POLICY

2026–2027

"Learning, Living, Loving together in Christ."

Approval	Governing Body
Date approved	22.10.2026
Review	Autumn 2027

1. Catholic Ethos, Purpose and Scope

At Our Lady and St Rose of Lima Catholic Primary School, every child is made in the image and likeness of God. Our mission, "Learning, Living, Loving together in Christ", underpins respectful and safe digital participation. Online safety is an integral part of safeguarding, not solely an ICT responsibility.

This policy applies to pupils from Nursery to Year 6, staff, governors, volunteers and visitors using school technology, accounts or services, and to online conduct outside school where it affects pupil safety or school life. It applies to school-owned and, where relevant, personal devices.

2. Statutory Framework and Related Policies

The school will follow current statutory requirements and relevant DfE guidance, including Keeping Children Safe in Education, Meeting Digital and Technology Standards in Schools and Colleges, Filtering and Monitoring Standards, Behaviour in Schools, and the statutory safeguarding and education duties under the Education Act 2002, Equality Act 2010, UK GDPR and Data Protection Act 2018. Current guidance takes precedence if updated during the policy year.

This policy must be read alongside: Safeguarding and Child Protection Policy 2026–2027; Pastoral and Positive Behaviour Policy 2026–2027; Anti-Bullying Policy 2026–2027; Mobile Phones, Smart Devices and Wearable Technology Policy; AI Acceptable Use Policy; SEND Policy; RSHE Policy; Computing Curriculum; Data Protection and Privacy Notices; Staff Code of Conduct; Acceptable Use Agreements; Complaints Policy; and Suspension and Permanent Exclusion Policy.

3. Understanding Online Risks — the Four Cs

- **Content**: exposure to harmful or illegal material, misinformation, pornography, extremist material, self-harm content and discriminatory material.
- **Contact:** grooming, coercion, unwanted communication, exploitation, impersonation and pressure from adults or peers.
- **Conduct**: online bullying, threats, harassment, harmful image-sharing, oversharing, identity misuse and harmful or abusive communications.
- **Commerce:** scams, phishing, fraud, gambling, inappropriate advertising, in-app purchasing and data exploitation.

Risks can overlap and may involve generative AI, manipulated imagery, gaming platforms, messaging, social media or emerging services. Staff consider age, SEND, vulnerability and the wider safeguarding context.

4. Responsibilities and Governance

- **Governing Body:** provides strategic oversight, receives regular anonymised reports, seeks assurance that filtering and monitoring arrangements are effective and that staff receive training.
- **Headteacher, DSL and Strategic Online Safety Lead (Mrs Hensman):** has overall accountability for online safeguarding, the school's online safety culture, resourcing, policy implementation, filtering and monitoring oversight, and the response to serious incidents. The Headteacher ensures safeguarding concerns are managed through the DSL team and recorded on CPOMS.
- **Designated Safeguarding Lead team (Mrs Hensman, Mrs Edgington and Miss Kavanagh):** leads safeguarding responses, including online child-on-child abuse, exploitation, harmful sexual behaviour and referrals to external agencies where required.
- **Computing Subject Leader** — Operational Online Safety Curriculum Lead: leads the progression and delivery of online safety education through Computing and the wider curriculum, coordinates awareness activities and supports staff with teaching resources. Works with the Headteacher/DSL team and technical provider; safeguarding decisions and referrals remain the responsibility of the DSL team.
- **Technical and service providers:** Exa supplies internet connectivity and internet filtering directly to the school (not through Entrust). Securus supplies the monitoring system on a self-service basis; it does not review alerts on

the school's behalf. Mrs Hensman (Headteacher and DSL) is the primary reviewer of Securus alerts. Mrs Edgington (Deputy Headteacher and Deputy DSL) provides safeguarding cover when Mrs Hensman is unavailable. Mr Ingram also has Securus access and can support monitoring and technical follow-up. Any alert suggesting a safeguarding concern must be brought promptly to the DSL or Deputy DSL; technical access does not transfer responsibility for safeguarding decisions. Relevant pupil incidents and actions are recorded on CPOMS.

- All staff: model safe practice, supervise pupil access, follow acceptable use rules, report concerns immediately and record significant incidents factually on CPOMS.
- Pupils and families: follow age-appropriate expectations, report concerns and work with school to promote safe and respectful use.

5. Reporting, Safeguarding and CPOMS

Any member of staff who becomes aware of an online safety concern must secure immediate safety, listen without promising secrecy and report safeguarding concerns directly and without delay to a DSL. Staff must not wait for a CPOMS entry to be read. Significant incidents, actions, communications, decisions and follow-up must be recorded promptly and factually on CPOMS, with appropriate restricted access.

Where a child may be at immediate risk, staff follow the Safeguarding and Child Protection Policy, including emergency services or children's social care as necessary. Staff must not conduct their own investigation into suspected criminal material, groomers or serious child-on-child sexual harm; the DSL coordinates risk assessment, evidence preservation and external advice/referrals.

For nude or semi-nude images involving children, staff must not ask children to forward images, copy or share them, or intentionally view them. They must follow current UKCIS/DfE guidance and refer immediately to the DSL. Any inadvertent viewing or receipt is reported and handled under safeguarding procedures.

6. Online Bullying, Discrimination and Behaviour

Online bullying is addressed through the Anti-Bullying Policy and classified as Level 3 serious behaviour under the Pastoral and Positive Behaviour Policy. A single serious incident of discriminatory abuse, threats, sexual harassment or harmful image-sharing may warrant Level 3 and safeguarding action even where the definition of repeated bullying is not met.

Responses prioritise protection of those harmed, fact-finding, reasonable adjustments, proportionate consequences, pastoral support and review. The school may respond to off-site online behaviour within its lawful powers and the published Behaviour Policy. Restorative approaches must be voluntary, safe and never replace safeguarding action.

7. Filtering, Monitoring and Cybersecurity

The school uses Exa for internet connectivity and filtering and Securus for self-service monitoring. Mrs Hensman (Headteacher and DSL) is the primary Securus alert reviewer and checks alerts on every school day. Mrs Edgington (Deputy Headteacher and Deputy DSL) undertakes the school-day review when Mrs Hensman is unavailable. James Ingram also has Securus access to provide monitoring and technical support; safeguarding decisions remain with the DSL team. Alerts indicating potential harm are assessed and escalated promptly, with relevant concerns and actions recorded on CPOMS. The school will review monitoring patterns and responses termly and formally review filtering and monitoring effectiveness at least annually. During school holidays and periods of full school closure, school devices are not expected to be in use on the school premises. Consequently, Securus monitoring alerts are not normally expected to be generated, and routine daily monitoring checks will not be undertaken during these periods. Where school-managed devices remain in use, including remotely, or where there is a known safeguarding risk requiring continued monitoring, the Headteacher will review the arrangements and establish appropriate monitoring and escalation procedures. Any safeguarding concern brought to the school's attention during a closure will be addressed in accordance with the school's Safeguarding and Child Protection Policy. These arrangements will be reviewed annually, or sooner if there are changes to device usage, monitoring systems or safeguarding risks. Exa and Securus will be contacted as appropriate for technical issues. Filtering must block harmful content without unreasonably restricting educational access.

- Complete and document at least an annual review of filtering and monitoring effectiveness, including changing pupil needs, SEND and emerging risks.
- Maintain secure accounts, individual logins, strong authentication where appropriate, least-privilege access, prompt updates, malware protection, backups and technical incident procedures.
- Staff must not bypass safeguards or permit unsupervised access to unsuitable sites. Requests for educational exceptions require documented approval and risk assessment.
- Report suspected data breaches or cybersecurity incidents immediately to the Headteacher/authorised IT lead and DPO; follow breach reporting requirements, including ICO notification where legally required.

8. Teaching, Curriculum and Pupil Voice

Online safety is explicitly taught through Computing, RSHE, assemblies, pastoral provision and wider curriculum opportunities, and reinforced when digital tools are used. Teaching covers privacy, personal information, passwords, consent, respectful communication, recognising manipulation and misinformation, reporting, scams, online relationships, gaming, screen habits and age-appropriate AI literacy.

Teaching is adapted for EYFS, SEND and pupils with additional vulnerabilities. Pupils are taught how to seek help from trusted adults. Pupil voice, incident patterns and family feedback inform curriculum priorities.

9. Mobile Devices, Images and Communication

Use of phones, smart watches, personal devices and wearable technology is governed by the school's Mobile Phones, Smart Devices and Wearable Technology Policy. Staff communicate with families and pupils only through authorised school channels and must not use personal social media or messaging accounts for professional pupil contact.

Images or recordings of children must be taken, stored and shared only through approved school arrangements and in accordance with the school's privacy notices, permissions, safeguarding requirements and data protection procedures. Staff must not use personal devices to capture pupil images for school purposes unless specifically authorised under a documented exception. Families are reminded to respect the privacy and safeguarding needs of other children when recording school events.

10. Artificial Intelligence and Emerging Technology

The AI Acceptable Use Policy governs generative AI and automated services. Staff must not enter identifiable or confidential pupil, parent or staff information, or upload pupil photographs, recordings or safeguarding records, into unapproved AI systems. Any school-approved processing of personal data requires appropriate data protection and safeguarding checks. Pupil use of AI is supervised, age-appropriate and limited to approved educational purposes.

AI-generated impersonation, fabricated images, sexualised deepfakes, threats or manipulated content are treated as potential safeguarding incidents and, where applicable, serious behaviour or bullying incidents. Staff refer concerns to the DSL and avoid unnecessary viewing, copying or distribution.

11. Staff Conduct, Social Media and Acceptable Use

Staff must maintain professional boundaries online, protect confidential information, use school-approved accounts and systems, report accidental exposure or misuse promptly and follow the Staff Code of Conduct and Acceptable Use Agreement. Allegations concerning adults working with children must follow the Safeguarding and Child Protection Policy and relevant allegations/low-level concerns procedures, not an informal IT investigation.

12. Parents, Carers and Community

The school will provide practical online safety information through newsletters, parent communications and events, including reporting routes, age ratings, privacy settings, harmful content and emerging risks. Parents should contact the school promptly if online conduct affects a child's welfare or school life. Serious concerns will be handled sensitively and in accordance with safeguarding and confidentiality duties.

13. Monitoring, Training and Review

Service boundaries: Entrust provides FSM Checker, the VoIP telephone system and The Launch (BGFL365). Schools ICT provides SIMS support. These services must not be described as the school's internet filtering or Securus monitoring provision. Any safeguarding issues arising through these systems must follow the school's safeguarding and CPOMS procedures.

Staff and governors receive appropriate induction and regular online safety updates. Leaders monitor CPOMS incident patterns, filtering and monitoring reports, staff training, pupil voice, curriculum coverage and any relevant safeguarding themes. The governing body receives anonymised oversight information. This policy is reviewed at least annually and sooner following significant incidents, legal changes or emerging risks.

Appendix A — Online Safety Incident Response Flowchart

This decision pathway applies to pupil and staff concerns. Safeguarding action must not be delayed while an incident is recorded.

1. CONCERN IDENTIFIED

A child discloses; a member of staff observes harmful content or behaviour; or Exa/Securus identifies a concern.

2. MAKE SAFE

Protect the child; stop further exposure where safe; do not promise confidentiality or investigate suspected criminal material.

3. SAFEGUARDING RISK?

If immediate danger: contact emergency services and notify the DSL. If any child protection concern: speak directly to the DSL without delay.

4. DSL-LED RESPONSE

DSL assesses risk, child voice and support needs; considers police/children's social care advice and safe evidence preservation. For intimate images of children, do not request, copy, forward or intentionally view the images.

5. RECORD AND ACT

Record significant concerns, decisions, referrals and follow-up factually on CPOMS. Apply Behaviour/Anti-Bullying procedures where relevant, without substituting sanctions for safeguarding.

6. FOLLOW UP

Support affected children, inform families where safe and appropriate, review technical controls, and monitor recurrence.

Technical-only incidents without a safeguarding element should be reported to James Ingram or the authorised IT contact, with DSL escalation if a child protection risk emerges.

Appendix B — Pupil Online Safety Incidents and Responses

The following examples are guidance, not automatic sanctions. The school's Pastoral and Positive Behaviour Policy determines behaviour levels; the Safeguarding and Child Protection Policy takes precedence whenever a child may be at risk.

Accidental access to unsuitable content

Reassure and remove exposure; tell teacher; report filtering issue to technical support. Notify DSL and record on CPOMS if content or circumstances raise safeguarding concerns.

Minor inappropriate use of school technology

Re-teach acceptable use and supervise access; consider Level 1 or 2 according to context and repetition. Escalate persistent patterns.

Repeated misuse, password sharing or attempts to bypass filtering

Secure accounts/devices; involve technical support; consider Level 2 or 3 depending on risk, intent and impact; inform parents as appropriate; CPOMS for significant/persistent concerns.

Online bullying, targeted threats or discriminatory harassment

Protect pupils; inform SLT/DSL as appropriate; treat bullying as Level 3; record on CPOMS; follow Anti-Bullying Policy, with support for all children affected.

Grooming, coercion, exploitation or harmful sexual communication

Immediate DSL referral; assess safety and external referral needs; do not conduct an independent investigation; record and coordinate support through CPOMS.

Nude/semi-nude images of children, including AI-manipulated imagery

Immediate DSL referral; do not ask to see, copy, share, print or delete material without specialist DSL advice; follow safeguarding procedures and relevant guidance.

AI-generated impersonation, deepfakes or misuse of personal data

Protect affected children; assess safeguarding and data protection implications; involve DSL, technical lead and DPO as relevant; apply proportionate behaviour response.

Where conduct occurs outside school, any disciplinary response must remain within the school's lawful powers, as set out in the Behaviour Policy. Reasonable adjustments and SEND needs must be considered.

Appendix C — Staff Online Safety Incidents and Responses

Staff incidents are handled under the Safeguarding and Child Protection Policy, Staff Code of Conduct, acceptable use requirements, data protection procedures and relevant employment processes. This appendix does not prescribe disciplinary outcomes.

Accidental access to unsuitable material or suspicious messages

Stop access, do not interact further, report promptly to the authorised technical contact; notify DSL if children or safeguarding are involved.

Inappropriate personal use of school systems or breaches of acceptable use

Report to line manager/Headteacher; establish facts proportionately and consider technical restrictions, guidance, training or formal action as appropriate.

Loss, disclosure or insecure handling of personal information

Contain where safe; notify Headteacher and DPO promptly; follow data breach procedures and assess any required ICO/individual notification.

Unprofessional communication with pupils or families; inappropriate social media contact

Notify Headteacher/DSL promptly; preserve relevant evidence lawfully; consider staff conduct, safeguarding and allegations procedures.

Concern or allegation that an adult may have harmed a child, or poses a risk of harm

Follow the school's allegations-against-staff procedures immediately; Headteacher seeks LADO advice where the threshold is met. If concern relates to Headteacher, report to Chair of Governors as specified in safeguarding policy.

Suspected illegal content, child sexual abuse material, grooming or serious cybercrime

Do not investigate, download, copy or circulate suspected illegal imagery; notify DSL/Headteacher immediately and seek police/appropriate safeguarding advice. Preserve devices safely as advised.

Filtering/monitoring failure or security compromise

Notify James Ingram and Headteacher; implement safe containment, assess child safeguarding impact and inform Exa/Securus or other provider as appropriate.

Records must be restricted to those with a legitimate need to know. Child safeguarding concerns are recorded on CPOMS; staff personnel matters and data protection incidents are also managed through the appropriate confidential systems.

Approval and Review

Approving body	Governing Body
Date approved	To be confirmed
Chair of Governors signature	_____
Next review	Autumn 2027