Cyber Incident Response Plan

School: St Maria Goretti Catholic Primary School

Designated Incident Lead: Headteacher – Mrs Amanda Rich

Date: 31 August 2025

Review Date: July 2026 (or following incident)

This plan outlines the response to a suspected or confirmed cyber security incident. Its purpose is to ensure a swift, calm, and effective reaction to minimise disruption, data loss, and harm to pupils or staff.

1. Key Roles and Responsibilities

As a single-form entry school, individuals may hold multiple roles. The key is to understand the function required at each stage.

Role	Lead Person	Named Lead	Key Responsibilities
Incident Lead	**Headteacher**	Amanda Rich	• Has overall strategic command of the incident. • Makes key decisions (e.g., disconnecting systems, reporting to authorities) • Liaises with the Chair of Governors, Local Authority and Trust. • Leads the post-incident review.
Safeguarding Lead	**Designated Safeguarding Lead (DSL)**	Amanda Rich Laura Milne Lynn Taylor	• Assesses the immediate and potential risk of harm to children. • Determines if pupil data (especially for vulnerable children) has been compromised. • Advises the Incident Lead on safeguarding implications and reporting duties.
Technical Lead	**External IT Support Provider**	Ryan Green EasyTech solutions ltd MARCH 26 –Virtue Jason Carr	• Provides technical analysis of the incident. • Works to contain the threat and isolate affected systems. • Eradicates the cause of the incident. • Recovers systems and restores data from backups.

Communications & Operations Lead	**School Business Manager / Senior Admin Officer**	Mrs Karen Johnson April 26 Mrs Danielle Piccolo Gardiner	• Manages internal communications to staff • Prepares and sends approved communications to parents/carers • Liaises with key data processors (e.g., MIS, payments, comms providers). • Manages operational issues (e.g., if systems are down).
Governance	**Chair of Governors**	Christine wilson	• Is kept informed of the incident by the Headteacher. • Provides support and oversight without directing the operational response. • Ensures the school fulfils its statutory duties.

2. Cyber Incident Response

Phase 1: IDENTIFY & REPORT (First 30 Minutes)

- A Staff Member or System Alert IDENTIFIES a potential incident.
  - *(e.g., Ransomware message, unusual pop-ups, can't access files, phishing email has been clicked)*
  - **Action:** Do not switch off the computer unless instructed. Disconnect it from the network (unplug the ethernet cable or turn off Wi-Fi).
- IMMEDIATE REPORT to the Headteacher (Incident Lead) and DSL.
  - **Action:** Staff member provides a clear account of what they saw and did.

Phase 2: ASSESS & CONTAIN (First 1-2 Hours)

- Headteacher convenes the core response team (Headteacher, DSL, SBM).
- Headteacher contacts the EXTERNAL IT SUPPORT PROVIDER (Technical Lead).
  - **Responsibility:** Headteacher.
  - **Action:** Provide all known details. Follow their immediate instructions.
- IT Support investigates and advises on CONTAINMENT.
  - **Responsibility:** IT Support.
  - **Action:** May advise isolating the school network from the internet, shutting down servers, or taking specific systems offline.
- DSL assesses the safeguarding risk.
  - **Responsibility**: DSL.
  - **Action:** Is there a risk of harm to children? Has personal data been accessed, especially for vulnerable pupils?

Phase 3: RESOLVE & RECOVER (Hours to Days)

- IT Support works to ERADICATE the threat.
  - Responsibility: IT Support.
  - **Action:** Remove malware, block malicious connections, patch vulnerabilities.
- IT Support begins RECOVERY.
  - Responsibility: IT Support.
  - **Action**: Restore systems and data from clean, recent backups. Verify data integrity.
- School team tests key systems before bringing them fully back online.
  - **Responsibility:** SBM / Admin Team.

Phase 4: COMMUNICATE & REPORT (As Required, some within 72 hours)

- Headteacher decides if a personal data breach has occurred.
  - **Responsibility:** Headteacher (with advice from DSL and IT Support).
- IF a significant personal data breach has occurred:
  - Report to the Information Commissioner's Office (ICO) within 72 hours.
    - **Responsibility:** Headteacher.
- Report the crime.

    - Report to Action Fraud.
        - **Responsibility:** Headteacher / SBM.
- Notify other key bodies.
    - Inform the Department for Education (DfE).
    - Inform Local Authority
        - **Responsibility:** Headteacher.
- Manage Communications.
    - Communicate with staff about the status and what they can/cannot do.
    - Communicate with parents/carers if their data is affected or if school operations are impacted. All communications must be approved by the Headteacher.
        - **Responsibility**: SBM (drafting), Headteacher (approving).

Phase 5: REVIEW & LEARN (1-2 Weeks Post-Incident)

- Incident Lead convenes a full review meeting.
    - **Responsibility:** Headteacher.
    - **Attendees:** DSL, SBM, IT Support, Chair of Governors.
- Review the response: What went well? What could be improved?
- Identify lessons learned: What vulnerabilities were exploited?
- Action Plan: Update policies, implement new security measures, and plan staff training.

3. Key Contacts & Resources

Service	Contact Details
External IT Support Provider	ryan@easytech-it.co.uk Ryan Green IT technician 07801282116
Local Authority / Trust Contact	Samantha Oates 07813 575568 samantha.oates2@lancashire.gov.uk Luke Capper lcapper@mecmat.org
Chair of Governors	Christine Wilson cwilson@stmariagoretti.mecmat.org
Information Commissioner's Office (ICO)	Helpline 0303 123 1113 https://ico.org.uk/for-organisations/report-a-breach/
Action Fraud	**Helpline** 0300 123 2040 actionfraud.police.uk
DfE Sign-in Service	https://services.signin.education.gov.uk/ (to report a breach to the DfE)
National Cyber Security Centre (NCSC)	For guidance and support: ncsc.gov.uk