



QE Cyber Security Incident Response Policy

Academic Year 2026-27

	Name	Title	Date
Prepared by	Harikumar Rajagopal	Global Senior IT Manager	30/06/2026
Reviewed by	Daksh Singhal	Group Head of Operations	30/06/2026
Approved by	Governing Body		10/07/2026
Next review	August 2027		

Table of Contents

1. Purpose	3
2. Scope	3
3. Incident Response Principles	3
4. Incident Classification.....	4
5. Incident Response Process.....	4
6. Roles & Responsibilities	5
6.1 IT Department	5
6.2 Staff Members.....	5
6.3 School Leadership	5
7. Compliance	6

1. Purpose

The purpose of this policy is to establish a consistent approach for identifying, reporting, responding to and recovering from cyber security incidents affecting Queen Elizabeth's School technology services and information assets.

The policy aims to minimise the impact of cyber security incidents, protect School information and ensure the timely restoration of normal operations

2. Scope

This policy applies to:

- All employees.
- Students.
- Contractors and consultants.
- Third-party service providers.
- Any individual authorised to use School technology resources.

This policy applies to all School technology services including:

- Microsoft 365.
- Email services.
- Network infrastructure.
- Cloud services.
- Business and educational applications.
- End user computing devices.
- Cyber security systems.
- Digital information and records.

Where local legal or regulatory requirements differ, country-specific requirements shall take precedence.

3. Incident Response Principles

Information Technology within Queen Elizabeth's School shall be governed using the following principles:

- Support teaching, learning and business operations.
- Protect School information and technology assets.
- Deliver secure, reliable and resilient technology services.

- Ensure technology is available to authorised users when required.
- Promote responsible, ethical and professional use of technology.
- Comply with applicable legal, regulatory and contractual requirements.
- Manage technology risks through appropriate governance and security controls.
- Continuously improve technology services to meet organisational needs.

4. Incident Classification

Cyber security incidents may include, but are not limited to:

- Malware or ransomware infections.
- Phishing or social engineering attacks.
- Unauthorised access to systems or information.
- Compromise of user accounts.
- Data loss or data breaches.
- Denial of Service (DoS) attacks.
- Loss or theft of School devices containing School information.
- Any suspected activity that could affect the confidentiality, integrity or availability of School information or technology services.

Incidents shall be assessed and prioritised based on their impact and urgency.

5. Incident Response Process

The School shall follow a structured response process:

Identification

- Identify and report suspected cyber security incidents.
- Record relevant information.

Assessment

- Assess the nature, impact and severity of the incident.
- Determine the appropriate response.

Containment

- Take appropriate action to limit the impact of the incident.
- Protect affected systems and information.

Recovery

- Restore affected services safely.
- Verify that systems are operating normally before returning to service.

Review

- Document the incident.
- Identify lessons learned.
- Implement improvements where required.

6. Roles & Responsibilities

6.1 IT Department

The IT Department is responsible for:

- Managing cyber security incidents.
- Coordinating investigation and response activities.
- Protecting affected systems.
- Restoring technology services.
- Maintaining incident records.
- Recommending security improvements.

6.2 Staff Members

Staff members are responsible for:

- Reporting suspected cyber security incidents immediately.
- Following guidance provided by the IT Department.
- Protecting School information during an incident.
- Cooperating with incident investigations where required.

6.3 School Leadership

School Leadership is responsible for:

- Supporting the incident response process.
- Providing appropriate business decisions during significant incidents.
- Supporting communication with relevant stakeholders where required.
- Reviewing significant incidents and improvement recommendations.

7. Compliance

All users are expected to report suspected cyber security incidents promptly and comply with this policy.

The Information Technology Department will periodically review the school's cyber security incident response arrangements to ensure they remain effective and aligned with organisational requirements.