Holy Trinity CE Junior School

Policy for:	**Cyber Security**
Written by:	**Judicium**
Date Adopted:	**Summer 2025**
Review Date:	**Summer 2027**

Motto	**Only with Thee, O God, we journey safely on**
Vision	Exemplary education for all, through God's amazing grace.
4 year Vision target:	By the end of July 2027**: attainment and progress will remain above or within the national average; children will retain their knowledge securely; children will confidently articulate Christian values, children will be proactive learners and have aspirations for what they can achieve in life; children recognise how to behave towards one another in everyone's best interests; children will know how to be healthy, safe and enjoy life to the full!**
Values	**Learning, Dignity, Integrity, Confidence, Love**
Values statement	**Learning together, as we journey with God in Love, we act with Integrity, treat others with Dignity and grow in Confidence.**
We Learn:	**"Everything was created through Jesus and for him" Colossians 1.16.** The sub values are: Curiosity, Wisdom, Teamwork, Hard Work and Failing Well
We Love:	**"We love each other because he loved us first" 1 John 4.19.** The sub values are: Community, being Non-judgmental, Forgiveness, Compassion and Kindness
We act with Integrity:	**"People judge by outward appearance, but the Lord looks at the heart" 1 Samuel 16.7.** The sub values are: Faithfulness, Generosity, Honesty, Trustworthiness, Self-Control and Responsibility
Each person has Dignity:	**Each person has Dignity: "So God created human beings in his own image." Genesis 1.27.** The sub values are: Equality, The Whole Person, Every Person, Tolerance and Advocacy
We have Confidence:	**We have Confidence: "Blessed are those who trust in the Lord and have made the Lord their hope and confidence." Jeremiah 17:7.** The sub values are: Wholeheartedness, Hopefulness, Joy, Humility and Resilience

Document Owner and Approval

Judicium is the owner of this document and the data manager and head teacher are responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff on R drive via the office staff.

Signature: Date:

Version History Log

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	19.10.21
2	Formatting amendments	03.08.22
3	Included details of cyber crime, technology solutions, controls and guidance for staff.	30.08.24 14.5.25

Introduction

Cyber security has been identified as a risk for the School and every employee needs to contribute to ensure data security.

The School has invested in technical cyber security measures but we also need our employees to be vigilant and to act to protect the School IT systems.

Cygnet / LGfL is responsible for cyber security within the School. Cygnet can be contacted via 020 8619 1200 or helpdesk@cygnet.it. LGfL can be contacted on 020 8408 4455.

If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy and Home Working Policy,

Purpose and Scope

The purpose of this document is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as to set out an action plan should the School fall victim to cyber-crime.

This policy is relevant to all staff.

What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- Cost – The global cost of all forms of online crime is estimated to be in excess of £300 billion. We may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data.
- Confidentiality and data protection - Protecting individuals' confidential information and all forms of personal data is one of the most essential requirements our school. The risk to confidential information and personal data is the biggest of all threats from cyber-crime.

- Potential for regulatory breach – We have various regulatory duties which we could unintentionally breach through falling victim to cyber-crime or a cyber-attack. Loss of personal data can lead to claims for damages by the individuals concerned and/or significant fines from the Information Commissioners Office (ICO).

- Reputational damage – A cyber security incident can have a major impact on our reputation, particularly if it involves the loss of confidential information, personal data and/or is reported in the media. Protecting our reputation is of utmost importance.

- Business interruption; Some forms of cyber-attack could render key systems (for instance servers including email servers, cloud computing services or our website) unavailable. This would have a major impact on delivering lessons and delivering our services. It may be necessary in such cases to invoke our Business Continuity Plan. SBM is responsible for making that decision and communicating with IT.

- structural and financial instability – The financial losses flowing from online crime may cause or contribute to financial difficulty.

Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for the School to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Data Manager can provide further details of other aspects of the School risk assessment process upon request.

The School have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

Technology Solutions

The School have implemented the following technical measures to protect against cyber-crime:

(i) firewalls;

(ii) anti-virus software;

(iii) anti-spam software;

(iv) auto or real-time updates on our systems and applications;

(v) URL filtering;

(vi) secure data backup;

(vii) encryption;

(viii) deleting or disabling unused/unnecessary user accounts;

(ix) deleting or disabling unused/unnecessary software;

(x) using strong passwords; and

(xi) disabling auto-run features.

Controls and Guidance for Staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.
- All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the School or any third parties with whom we share data.
- It may be appropriate in some instances to limit the number of people involved or who have access to information on a matter to ensure the security of the data involved. This can be part achieved through IT security measures. We may implement other controls that are more practical in nature, e.g.:
- Physically ringfencing the individuals or teams working on a matter;
- Taking steps to ensure our system for opening, distributing and/or scanning incoming correspondence (by post, email or otherwise) does not allow or inadvertent sharing of confidential information;
- Getting a signed confidentiality agreement from each staff member;

- Disposing of confidential documents securely;
- Having a clear desk policy;
- Discouraging staff from reading confidential papers or discussing sensitive matters in public.
- Due diligence – we may conduct due diligence on the cyber security controls and cyber-crime prevention measures that other parties with whom we share information.

All staff must:

- Choose strong passwords which will be changed regularly
- keep passwords secret;
- never reuse a password;
- staff must complete mandatory annual cyber training.
- never allow any other person to access the school's systems using your login details;
- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the School IT systems;
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to the Data Manager as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy;
- only access work systems using computers or phones that the School owns. Staff may only connect personal devices to the Wi-Fi provided;
- not install software onto your School computer or phone. All software requests should be made to the computing lead, Data Manager & the Head teacher

- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks.

The School considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against the School or using the School's systems;
- accessing inappropriate, adult or illegal content within School premises or using School equipment;
- excessive personal use of School's IT systems during working hours;
- removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy;
- using School equipment in a way prohibited by this policy;
- circumventing technical cyber security measures implemented by the School's IT team; and
- failing to report a mistake or cyber security breach.

Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages:

(i) *Containment and recovery:* To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost. We will notify our insurers as soon as reasonably practicable of any circumstances that may give rise to claim under relevant insurance policies. We will also assess whether it is necessary to invoke our business continuity plan.

(ii) *Assessment of the ongoing risk:* To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed and any consequences of the breach/attack identified.

(iii) *Notification:* To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.

(iv) *Evaluation and response:* To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber security incident involves a personal data breach, the School will invoke their Data Breach Policy rather than follow out the process above.

Appendix A

Cyber Management Plan

Holy Trinity CE Junior School
Last updated: July 2025
Next review: July 2027

1. Purpose

To define the process for preparing for, detecting, responding to, and recovering from cyber incidents that may impact school operations, in alignment with the school's Cyber Security Policy and Business Continuity Plan (BCP).

2. Governance

- **IT Partner:** Cygnet / LGfL (handles technical incident response)
- **BCP Coordination:** SBM (invokes BCP when cyber incidents disrupt core services)
- **Overall Lead:** Headteacher (final decision-maker in serious breaches)

3. Core Objectives

- Prevent unauthorised access, disruption, or destruction of systems/data.
- Minimise operational disruption caused by cyber incidents.
- Safeguard personal and sensitive data.
- Coordinate rapid recovery and communication in the event of an incident.

4. Prevention and Protection

Technical Measures (Per Cyber Security Policy):

- Firewall, antivirus, anti-spam, encryption, and backups
- URL filtering and disabling unused software/accounts
- Strong passwords and controlled admin access

Staff Measures:

- Regular cyber awareness training (at induction and refresher sessions)
- Clear expectations for IT use (e.g., no software installation without approval)
- Strong password hygiene
- Incident reporting protocol to the School Office Administrator

5. Incident Response Framework

A. Detection and Reporting

- All staff must report suspicious activity, phishing emails, or potential breaches to the School Office Administrator immediately.
- School Office Administrator logs the incident and evaluates severity with Cygnet / LGfL.

B. Initial Assessment

- Determine if incident involves:
    - Data breach (invoke **Data Breach Policy**)
    - Disruption to IT infrastructure (invoke **BCP**)
    - Reputational risk (notify Headteacher and Chair of Governors)

C. Containment and Mitigation

- IT team (Cygnet / LGfL) isolates affected systems.
- SBM determines if operations (e.g., registers, SIMS, communications) are affected.
- Backup systems activated if necessary (per Cyber Policy).

D. Escalation and Communication

- If core systems are compromised, Headteacher decides whether to:
    - Close school temporarily (see BCP snow/closure protocol)
    - Initiate remote learning
    - Notify staff via WhatsApp groups and Intouch
    - Communicate with parents via website and OpenCheck

E. Regulatory Notification

- Data breaches reported to ICO within 72 hours if required.
- Reported to National Crime Agency or DfE if deemed critical.

6. Recovery Procedures

Restoration Activities:

- Cygnet / LGfL restores systems using secure backups.
- SBM and Office Team assess readiness to resume normal operations.
- Notify stakeholders when systems are back online.

Post-Incident Actions:

- SLT evaluates root cause and identifies gaps.
- Policies and staff training reviewed and updated.
- Incident documented and logged for audit trail.

7. Alignment with Business Continuity Plan

Cyber events that trigger business disruption (e.g., no access to registers, communications failure, data loss) will invoke the BCP, specifically:

BCP Scenario	Cyber Risk Trigger	Response
No telephone/internet	Cyber attack on VoIP/email/SIMS	Use staff personal data or OpenCheck to post emergency info
Adverse weather/closure	IT disruption overlaps with physical inaccessibility	Remote learning via Teams/Google Classroom if systems safe

BCP Scenario	Cyber Risk Trigger	Response
Loss of power/data systems	Cyber breach causes shutdown	Notify Head + activate Grab Bag + paper registers
Email/phone threats	Phishing/social engineering attack	Evacuate/close school if threat credible (per BCP instructions)

8. Roles and Responsibilities Overview

Role	Responsibility
School Office Administrator	Incident logging, reporting, liaison with Cygnet / Judicium
Headteacher	Final decision-maker on school closure, communication
SBM	BCP coordination, resource allocation, grab bag access
Office Team	Communication with parents/staff, admin system backup
Cygnet / LGfL	Technical investigation and system recovery
All Staff	Incident reporting, policy adherence, safeguarding data

9. Review and Training

- Annual cyber drill simulation to test staff response and BCP triggers
- Update training materials after any real incident
- Policy reviewed every 2 years or post-incident