EDITH STEIN
CATHOLIC ACADEMY TRUST

CYBER SECURITY POLICY AND PROCEDURES

APPROVED BY DIRECTORS	**SEPTEMBER 26**
DATE LAST REVIEWED	**New**
MEMBER OF STAFF RESPONSIBLE	**Chief Executive Officer**
STATUTORY / NON-STATUTORY	**Non Statutory**

DRAFT

CONTENTS

Section	Heading	Page
1.0	Introduction	2
2.0	Scope	3
3.0	IT Technical Security Measures	4
4.0	Types of Cyber Attack	5
5.0	Confidential Data	6
6.0	Device Security	7
7.0	Access Control	9
8.0	Email and File Safety	10
9.0	Data Protection	11
10.0	Acceptable Use	12
11.0	Asset Management	13
12.0	Network Security	13
13.0	Vulnerability and Patch Management	14
14.0	Backup and Recovery	14
15.0	Physical Security	14
16.0	Third-Party Suppliers and Cloud Services	15
17.0	Security Awareness and Training	15
18.0	Remote and Home Working	15
19.0	Incident Reporting	16
20.0	Response Plan Outline	17
21.0	Response Plan Details	18
Appendix A	Supporting References	20
Appendix B	Incident Recovery Event Recording Form	21

DRAFT

1.0 Introduction

1.1 Edith Stein Catholic Academy Trust is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our approach to cyber security, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education guidance. *(See Appendix A)*

1.2 The purpose of this policy is to:

- Protect the confidentiality, integrity, and availability of our data and systems.
- Minimise the risk of cyber incidents.
- Ensure compliance with applicable laws, regulations, and standards.
- Promote a culture of security awareness and best practice.

Regardless of whether a school's IT infrastructure is managed directly by the Trust or through an approved third-party provider, the Trust retains strategic responsibility for ensuring that appropriate cyber security standards, controls and assurances are in place across schools and its core services

The Trust expects all schools and IT service providers to implement robust security measures that protect the confidentiality, integrity and availability of information and digital services. LGBs have a responsibility for monitoring IT systems at a local level; this includes compliance with relevant legislation, regulatory requirements, Trust policies and recognised cyber security standards. The Trust will establish minimum cyber security expectations, monitor compliance, assess risks, and seek assurance that effective arrangements are in place to prevent, detect, respond to and recover from cyber security incidents.

Where IT services are provided by a third party, the academy and Trust will ensure that contractual arrangements clearly define cyber security responsibilities, reporting requirements, and accountability for protecting Trust and school systems and data. All providers must demonstrate that they meet the Trust's cyber security requirements and support the Trust's commitment to continuous improvement in cyber resilience.

IT Manager refers to the appropriate member of staff or contractor engaged by the school

IT Department refers to the school IT department, contractor or company that manages the Trust or school's system

1.3 Responsibility and Accountability

Effective cyber security depends upon clear lines of responsibility and accountability. The Trust must ensure that responsibility for cyber security risks, controls and actions is clearly identified and understood at every level of the organisation, where relevant this is reflected in this policy. This includes establishing who is responsible for strategic oversight, operational management, technical controls, incident response, staff awareness and the management of individual systems and services.

Responsibilities should not be assumed simply because an individual or team has historically undertaken a particular task; they should be explicitly documented and communicated. Where responsibility is shared between the Trust, individual schools, external providers or other partners, the respective responsibilities of each party must be clearly defined, including who retains overall accountability. This clarity is essential to ensure that risks are identified and addressed promptly, actions are not overlooked, and there is clear ownership when responding to a cyber security incident.

1.4 Policy Requirements and ICT Outsourcing

Each section of this policy contains specific policy statements and, where appropriate, requirements for definite action within schools. These requirements are intended to provide a clear minimum standard for cyber security across the Trust and its schools. Schools should therefore use this document as a specification when procuring, commissioning or outsourcing ICT services or responsibilities to external providers. Where an external provider is responsible for delivering an ICT or cyber security function on behalf of a school, the school must ensure that the provider's responsibilities are clearly defined and that the service provided meets the requirements set out within this policy. Outsourcing a function does not transfer the school's accountability for ensuring that the relevant requirements are met, and appropriate contractual arrangements, service levels and assurance mechanisms should be in place to demonstrate compliance.

1.5 Other Policy documents

This policy is to be read in conjunction with ESCAT General ICT Policy, Data Protection Policy and Acceptable Use Policy.

2.0 Scope

2.1 This policy applies to:-

All staff, students, governors, and any third parties who have access to Edith Stein Catholic Academy Trust’s IT systems and data.

All devices (company-issued or personal) used to access company data or systems.

All IT systems, cloud services, and data owned or processed by the organisation.

The policy pertains to all school related systems and systems operated by the ESCAT to run

3.0 IT Technical Security Measures

3.1 *ESCAT* implement the following security measures, scaled to our size and needs:

Security Requirement	Control Standard
Firewall	Fortigate Firewall with UTM network security controls and filtering.
Anti Virus	Sophos Anti-Virus and Anti-Malware software on all devices.
Desktop operating systems	All school-owned devices imaged with Windows 11 or equivalent (e.g. MacOS).
Patching and updates	Software updates and patch management controlled via Datto RMM and Action1.
Backups	Daily Redstor secure data backups and termly tested recovery procedures.
Encryption	Data and emails across the Microsoft tenancy.
Encryption using portable devices	All school-owned portable devices fully encrypted using BitLocker
Multi-factor authentication	For critical systems and remote access. (Staff only).
Access control	Access control and permissions based on job roles and are reviewed regularly.
Cloud services	Secure configuration and monitoring of cloud services (e.g. Office 365).
Password Policy	Strong password policy in line with DFE guidelines. *(See Appendix A)*
Leavers	Prompt removal of access for leavers.
Penetration testing	Annual external penetration testing using external consultancy
Notifications	Police CyberAlarm installation and NCSC Early Warning reporting. *(See GDPR policy)*

3.2 Schools to record the implementation measures it uses against each criteria

Security Requirement	Control Standard
Firewall	
Anti Virus	
Desktop operating systems	
Patching and updates	
Backups	
Encryption	
Encryption using portable devices	
Multi-factor authentication	
Access control	
Cloud services	
Password Policy	
Leavers	
Penetration testing	
Notifications	

4.0 Types of Cyber Attack

The below table indicates, but is not limited to, different types of cyber attacks.

DoS and DDoS attacks	*Designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service (DDoS) attack is similar in that it also seeks to drain the resources of a system.*
Man-in-the-middle (MITM)	*Breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers.*
Phishing attacks	*Malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target.*
Whale-phishing attacks	*Malicious actors who go after the "big fish" or whales of an organization, which typically include those in charge of the organisation. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.*
Spear-phishing attacks	*Attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant. Uses email spoofing, where the information inside the "From" portion of the email is faked, making it look like the email is coming from a different sender.*
Ransomware	*The victim's system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer.*
Password attacks	*Attack to figure out target's password. This can be achieved by; brute-force, end-users leaving password around locally, guess work of 'easy' default password formulas, or an attacker paying someone on the inside to obtain the password.*
Trojan horses	*Attack uses a malicious program hidden inside a seemingly legitimate one. When the user executes program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network.*
Malware attack	*Malware infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another*

	or remain in place, only impacting its host device.

5.0 Confidential Data

	Responsible Body - School	Responsible Body - Trust
5.1 Confidential data includes any personal, sensitive, safeguarding, financial, business, or operational information that could cause harm to the Trust, its staff, pupils, parents, governors, or the wider community if disclosed, altered, lost, or accessed without authorisation.	**IT Manager**	**CFO** **IT Manager**
5.2 Schools shall ensure that confidential and sensitive information is protected in accordance with UK GDPR, the Data Protection Act 2018, and other relevant statutory and regulatory requirements. *(See Appendix A).*	**LGB** **DPO**	**CFO**
5.3 All Trust-owned portable devices, including laptops, tablets, and other mobile devices must be encrypted using approved encryption technologies to protect data in the event of loss or theft.	**IT Manager**	**CFO** **IT Manager**
5.4 Documents and records containing confidential or sensitive information should be appropriately classified, clearly identified where necessary, and only accessible to authorised personnel with a legitimate business or educational need.	**Senior Leadership Team**	**CFO**
5.5 Confidential data must only be stored on approved Trust systems or devices, secure network locations, or authorised cloud services that meet the Trust's security and data protection requirements	**IT Manager**	**CFO**
5.6 The storage, processing, or transmission of confidential data using personal devices, personal email accounts, or unauthorised cloud storage services is prohibited unless expressly authorised by the school Senior Leadership Team and appropriate security controls have been implemented.	**Senior Leadership Team**	**CFO**
5.7 Staff must only use Trust approved methods for sharing confidential information. Where sensitive or special category data is transmitted electronically, appropriate security measures, including encryption where necessary, must be used.	**IT Manager**	**IT Manager**
5.8 Confidential data must not be accessed, stored, or transmitted using unsecured public Wi-Fi networks unless a Trust-approved secure connection, such as a Virtual Private Network (VPN), is in use. Users should exercise extreme caution when connecting Trust-owned devices to public or free Wi-Fi services provided by cafés, hotels, restaurants, airports, shopping centres, public transport providers, or other public venues.	**LGB**	**CFO**

5.9 The use of external removable storage devices, including USB flash drives and external hard drives, is discouraged and may only be used where there is a legitimate operational requirement and approval from the IT Department. Any approved device must be encrypted and regularly scanned for malware. School-owned SD cards and memory cards used within approved cameras, camcorders, or other media recording devices are exempt from encryption requirements where the device does not support encryption.	**IT Manager**	**IT Manager**
5.10 Printed documents containing confidential information must be stored securely when not in use and must not be left unattended in classrooms, offices, staff rooms, printers, photocopiers, or other shared areas. Confidential documents must be disposed of using approved confidential waste or secure shredding procedures.	**IT Manager** **DPO**	**CFO**
5.11 Any actual or suspected loss, theft, unauthorised disclosure, corruption, or compromise of confidential data must be reported immediately to the school Data Protection Officer (DPO) and IT Manager and CFO. All incidents shall be investigated in accordance with the Trust's Data Breach Response Procedures and reported to the Information Commissioner's Office (ICO) where required by law.	**IT Manager** **DPO**	**CFO**
5.12 Particular care must be taken when handling safeguarding records, SEND information, medical records, personnel files, and other special category data. Access to such information shall be restricted to authorised staff with a legitimate need to access it.	**IT Manager** **DPO**	**IT Manager**
5.13 Staff must verify recipient details before sending emails or sharing documents containing personal or confidential information to reduce the risk of accidental disclosure.	**IT Manager** **DPO**	**CFO**

6.0 Device Security

	Responsible Body - School	**Responsible Body - Trust**
6.1 All Trust-owned devices used to access Trust systems, networks, or data must be configured and maintained to protect against cyber threats, unauthorised access, and data loss.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
6.2 All portable devices, including laptops and tablets, must have full-disk encryption enabled using Microsoft BitLocker. Encryption recovery keys shall be stored securely and may only be accessed by authorised IT Support staff for legitimate recovery purposes.	**IT Manager** **IT Department**	**IT Manager** **IT Department**

6.3 All devices must be protected with antivirus and anti-malware software, installed and approved by the IT department, and receive regular security updates. Operating system updates, software patches, and security policies shall be deployed and monitored through the Trust's Remote Monitoring and Management (RMM) system, where applicable.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
6.4 Devices shall be configured to automatically lock after a period of inactivity. Users are responsible for manually locking their device whenever it is left unattended, regardless of location.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
6.5 The school IT Department or support team shall maintain and enforce the Trust's Password Policy. Staff passwords must be changed at least annually and must not be re-used within a five-year period. Passwords must be a minimum of 12 characters in length and contain a combination of letters and numbers, or use an approved passphrase format such as the 'What3Words' methodology.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
6.6 Passwords, PINs, Multi-Factor Authentication (MFA) codes, and other authentication credentials must not be shared with any other individual and must be kept secure at all times.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
6.8 Users must not download, install, or use unauthorised, suspicious, illegal, or unlicensed software on any Trust-owned device. All software installations must be approved by the IT Department.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
6.9 Local administrator rights shall be restricted to authorised IT personnel unless a specific operational requirement has been approved by the IT Manager.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
6.10 Devices must not be left unattended in unsecured locations and should be stored securely when not in use. Any loss or theft of a Trust-owned device must be reported immediately to the IT Department.	**IT Manager** **IT Department**	**CFO** **IT Manager**
6.11 Users must not disable, bypass, or interfere with security controls including antivirus software, web filtering, firewalls, endpoint protection, encryption, or monitoring systems.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
6.12 The IT Department reserves the right to remotely manage, monitor, restrict, lock, or wipe Trust-owned devices where necessary to protect Trust systems, data, users, or to respond to a security incident.	**IT Manager** **IT Department**	**IT Manager** **IT Department**

6.13 Any suspected malware infection, device compromise, unusual system behaviour, or security concern must be reported immediately to the IT Department for investigation.	**IT Manager IT Department**	**IT Manager IT Department**

7.0 Access Control

	Responsible Body - School	**Responsible Body - Trust**
7.1 Effective access control measures are essential to protect the Trust's information systems, devices, networks, applications, and data from unauthorised access, misuse, disclosure, alteration, or destruction. Access control measures ensure users access the systems, information, and resources necessary to their role and responsibilities. Examples of access control measures include, but are not limited to: • Unique user accounts for all. • Strong password requirements and password expiry policies. • Multi-Factor Authentication (MFA), where available, for cloud services, remote access, and privileged accounts. • Role-Based Access Control (RBAC), ensuring users receive only the permissions required to perform their duties. • Separate privileged administrative accounts for IT staff. • Automatic account disabling following staff departures, role changes, or prolonged inactivity. • Screen lock policies and automatic session timeouts. • Guest network segregation from internal school networks. • Physical access controls, including locked server rooms and secure communications cabinets. • Approval processes for granting, modifying, or removing access rights. • Regular auditing and review of user accounts, permissions, and privileged access. • Monitoring and logging of access to systems containing sensitive or confidential information. • Restrictions on removable media, software installation, and administrative privileges.	**IT Manager IT Department**	**CFO IT Manager IT Department**
7.2 Access to Trust systems, applications, and data shall be granted on the principle of least privilege and based on the user's role and operational requirements. Users shall only be provided with the minimum level of access necessary to perform their duties.	**IT Manager IT Department**	**IT Manager IT Department**
7.3 User accounts shall be created, modified, and removed through authorised procedures. Access rights shall be reviewed whenever an	**IT Manager IT Department**	**Human Resources**

individual's role changes and promptly removed when a member of staff, student, contractor, or third party leaves the Trust.		
7.4 Multi-Factor Authentication (MFA) shall be enabled for systems containing sensitive information and for remote access services wherever technically feasible.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
7.5 The IT Department shall conduct periodic audits of user accounts, permissions, and privileged access rights to ensure access remains appropriate and compliant with Trust requirements.	**IT Manager** **IT Department**	**IT Manager** **IT Department**
7.6 Users are responsible for maintaining the security and confidentiality of their login credentials. User accounts, passwords, authentication tokens, and MFA devices must not be shared with any other individual.	**IT Manager** **IT Department**	**CFO**
7.7 Passwords must comply with the Trust's Password Policy and should be unique, difficult to guess, and changed immediately if compromise is suspected. (*see 6.5*)	**IT Manager** **IT Department**	**CFO**
7.8 Remote access to Trust systems shall only be permitted through approved and secure access methods. Users must not access Trust resources through unsecured public networks without appropriate security measures being in place. (see 5.8)	**IT Manager**	**CFO**
7.9 The Trust reserves the right to suspend, restrict, or revoke access to systems and data where there is a suspected security risk, policy breach, safeguarding concern, or operational requirement.	**LGB** **SLT** **IT Manager**	**CEO**
7.10 All access to systems, applications, and network resources may be logged and monitored for security, safeguarding, investigative, and compliance purposes in accordance with relevant legislation and Trust policies.	**IT Manager**	**IT Manager**

8.0 Email and File Safety

	Responsible Body - School	**Responsible Body - Trust**
8.1 Email remains one of the most common methods used by cyber criminals to distribute phishing messages, malware, ransomware, and other malicious content. All users must exercise caution when receiving emails, attachments, links, or file-sharing requests, particularly where the communication is unsolicited, unexpected, or originates from an unknown source.	**IT Manager** **IT Department**	**IT Manager**

8.2 Users must not open email attachments, download files, or click on hyperlinks unless they are satisfied that the sender is legitimate and the content has been verified as safe and relevant.	**School** **IT Manager** **IT Department**	**IT Manager**
8.3 Users must remain vigilant for signs of phishing, fraud, and social engineering attacks, including but not limited to: • *Unexpected requests for personal information, passwords, or financial details.* • *Messages creating a sense of urgency or pressure to act immediately.* • *Offers of prizes, gift cards, rewards, or other incentives.* • *Poor grammar, spelling mistakes, unusual formatting, or excessive punctuation.* • *Email addresses, display names, or domains that do not match the purported sender*	**School** **IT Manager** **DPO** **IT Department**	**CFO** **IT Manager**
8.4 Users must verify the legitimacy of requests involving payments, changes to bank details, disclosure of personal information, or sensitive data sharing through an alternative communication method before taking any action.	**IT Manager** **DPO**	**CFO**
8.5 Files received via email, file-sharing platforms, removable media, or other external sources must only be opened where there is a legitimate business or educational requirement, and the source is trusted.	**IT Manager**	**IT Manager**
8.6 Users must not bypass Microsoft 365 security controls, email filtering systems, antivirus protection, or any other security measures implemented by the Trust or their school.	**IT Manager**	**IT Manager**
8.7 Any suspected phishing email, malicious attachment, suspicious link, or potential security threat must be reported immediately to the IT Department. Users should not forward suspicious emails to other staff or students unless instructed to do so by the IT Department.	**IT Manager** **IT Department**	**IT Manager**
8.8 Trust schools will implement appropriate email security controls, including spam filtering, malware scanning, attachment protection, and where possible, Multi-Factor Authentication (MFA) to reduce the risk of email-based attacks.	**IT Manager** **IT Department**	**CFO** **IT Manager**
8.9 Staff handling personal, confidential, safeguarding, or special category data must ensure that information is only shared with authorised recipients and that appropriate security measures, including encryption where necessary, are used when transmitting data electronically.	**School**	**CFO** **IT Manager**
8.10 Users must take particular care when communicating with parents, pupils, governors, external agencies, and suppliers,	**School** **DPO**	**CFO** **IT Manager**

ensuring that recipient addresses are checked carefully before sending emails containing personal or sensitive information.		

9.0 Data Protection

	Responsible Body - School	Responsible Body - Trust
9.1 Edith Stein Catholic Academy Trust acknowledges the importance of safeguarding personal, sensitive and business data from loss, theft, or corruption.	**DPO**	**CEO** **CFO**
9.2 Across the Trust, personal and sensitive information shall be processed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant guidance issued by the Information Commissioner's Office (ICO). *(See ESCAT GDPR Policy)*	**DPO**	**CFO**
9.3 Data shall be automatically encrypted, where appropriate, including on portable devices (e.g. laptops and removable media), backups, and during electronic transmission.	**IT Manager** **IT Department**	**IT Manager**
9.4 The Trust will collect, process, and retain only the minimum amount of personal data necessary for legitimate educational, safeguarding, operational, and legal purposes. Data shall be retained in accordance with the Trust's Data Retention Schedule.	**DPO**	**CFO**
9.5 Access to personal data shall be restricted to authorised users. User permissions shall be reviewed regularly and removed promptly when staff leave or change roles.	**IT Manager** **IT Department**	**Human Resources**
9.6 Staff must not store personal or sensitive school data on personal devices, personal cloud storage services, or unauthorised applications.	**School**	**CFO**
9.7 Personal data shared with third parties shall only be disclosed where there is a lawful basis to do so and appropriate data sharing agreements or contractual safeguards are in place in accordance with the Trust GDPR policy. *(See Appendix 1)*	**School** **DPO**	**CFO**

10.0 Acceptable Use

	Responsible Body - School	Responsible Body - Trust
10.1 To promote the safe, secure, and responsible use of the Trust's information systems, networks, devices, and internet services, all staff and students are required to read, understand, and sign the	**School**	**CFO**

Trust's Acceptable Use Policy upon joining the school or Trust.		
10.2 Users shall use Trust-provided systems, devices, and network resources primarily for educational and business purposes and in a manner that is consistent with the Trust's values, policies, and legal obligations.	**School**	**CFO**
10.3 Users must not use Trust systems, networks, or devices for any illegal, inappropriate, offensive, discriminatory, or unauthorised activities.	**School**	**CFO**
10.4 Users must not install, download, or use unauthorised software, applications, browser extensions, or other tools without prior approval from the IT Department.	**School**	**CFO**
10.5 Users must not access, download, create, store, or distribute content that is illegal, harmful, offensive, or otherwise inappropriate within an educational environment.	**School**	**CFO**
10.6 Users must exercise caution when accessing websites, opening email attachments, or clicking links and must immediately report any suspected phishing attempts, malware, or suspicious activity to the IT Department.	**School**	**CFO**
10.7 Trust devices, accounts, and network credentials must not be shared with other individuals. Users are responsible for all activity conducted using their accounts and must take reasonable steps to protect their passwords and authentication methods. Passwords must not be disclosed, written down in unsecured locations, or reused across multiple systems. Passwords must not be shared. Users must immediately report any suspected compromise of their account to the IT Department.	**School**	**CFO**

11.0 Asset Management

	Responsible Body - School	**Responsible Body - Trust**
11.1 The Trust shall maintain an inventory of all IT assets, including servers, desktops, laptops, tablets, mobile devices, network equipment, software, and cloud services.	**LGBs**	**CFO**
11.2 All IT assets shall have an identified owner and be managed throughout their lifecycle, including procurement, deployment, maintenance, and secure disposal.	**LGBs**	**IT Manager**

12.0 Network Security

	Responsible Body - School	Responsible Body - Trust
12.1 The Trust and all schools shall implement appropriate network security controls, including firewalls, web filtering, intrusion prevention where applicable, and network segmentation.	**IT Manager**	**IT Manager**
12.2 Network infrastructure shall be configured and maintained by authorised IT personnel only. (Task)	**IT Manager**	**IT Manager**
12.3 Wireless networks shall be secured using approved encryption standards and access controls.	**IT Manager** **IT Department**	**IT Manager**

13.0 Vulnerability and Patch Management

	Responsible Body - School	Responsible Body - Trust
13.1 The Trust shall maintain a programme of vulnerability management to identify, assess, and remediate security weaknesses.	**IT Manager**	**CFO**
13.2 All Trust school are expected to apply critical security updates and patches shall be applied within an appropriate timeframe based on risk and operational requirements.	**IT Manager**	**IT Manager**
13.3 Regular vulnerability scans and security reviews must be undertaken to identify emerging threats.	**IT Manager**	**IT Manager**

14.0 Backup and Recovery

	Responsible Body - School	Responsible Body - Trust
14.1 The Trust shall maintain regular backups of critical systems and data.	**IT Manager**	**IT Manager**
14.2 Backup copies shall be protected from unauthorised access, stored securely, and tested termly to ensure successful recovery.	**IT Manager**	**IT Manager**
14.3 Restoration procedures shall form part of the Trust's business continuity arrangements.	**IT Manager**	**IT Manager**

15.0 Physical Security

	Responsible Body - School	Responsible Body - Trust
15.1 Access to server rooms, communications cabinets, and other critical IT infrastructure shall be restricted to authorised IT Department personnel.	**IT Manager**	**IT Manager**
15.2 Devices containing Trust data must be physically secured when not in use.	**School** **IT Manager**	**CFO**
15.3 Visitors shall not be permitted unsupervised access to areas containing critical IT infrastructure.	**School**	**CFO**

16.0 Third-Party Suppliers and Cloud Services

	Responsible Body - School	Responsible Body - Trust
16.1 All third-party software, cloud services, and suppliers that process Trust data shall be subject to appropriate security, safeguarding, and data protection assessments.	**IT Manager** **DPO**	**CFO**
16.2 The Trust shall ensure that suppliers handling personal data provide adequate technical and organisational security measures.	**DPO**	**CFO**

17.0 Security Awareness and Training

	Responsible Body - School	Responsible Body - Trust
17.1 All staff shall receive regular cyber security and data protection awareness training.	**School**	
17.2 Training shall include phishing awareness, password security, data handling, safeguarding considerations, and incident reporting procedures.	**School**	
17.3 Staff may be required to participate in periodic phishing simulations and security exercises.	**IT Manager**	

18.0 Remote and Home Working

	Responsible Body - School	Responsible Body - Trust
18.1 Users accessing Trust systems remotely shall only do so using Trust-approved devices and secure access methods.	**IT Manager**	**IT Manager**
18.2 Trust data must not be stored on personal devices or shared with unauthorised individuals.	**School**	**IT Manager**
18.3 Reasonable steps must be taken to prevent unauthorised viewing of sensitive information whilst working remotely.	**School**	**IT Manager**

19.0 Incident Reporting

	Responsible Body - School	Responsible Body - Trust
19.1 All staff, students, governors, contractors, and other stakeholders must report any suspected cyber security incident, phishing attempt, suspicious email, malicious link, malware infection, unauthorised access, or potential data breach to the IT Department immediately upon discovery.	**IT Manager**	**CFO**
19.2 Upon receiving a report, the IT Department shall assess the incident, record the relevant details, and determine the appropriate escalation route. Where necessary, notifications shall be issued to affected users, the Senior Leadership Team, Local Governing BODY the Data Protection Officer (DPO), or external authorities. The Trust CFO must be informed.	**SLT** **DPO** **IT Manager** **LGB**	**CFO**
19.3 The IT Manager shall proactively monitor security alerts, threat intelligence sources, and system monitoring tools to identify emerging threats that could affect the Trust's systems, users, or data.	**IT Manager**	**CFO**
19.4 The IT Department shall remain informed of relevant cyber security advisories, vulnerabilities, incidents, and best practice guidance issued by recognised bodies, including the Department for Education (DfE), National Cyber Security Centre (NCSC), Information Commissioner's Office (ICO), and technology providers.	**IT Manager** **DPO** **IT Department**	**CFO**
19.5 Any user who believes that their account, device, password, or personal information may have been compromised must report the matter immediately to the IT Department.	**IT Manager**	**CFO**
19.6 The method by which the Trust becomes aware of a cyber security incident may affect its severity, priority, and reporting requirements. Incidents may be identified through, but are not limited to, the following sources: • *Discovery through IT Department monitoring, alerting, or security systems.*	**LGBs** **SLT** **DPO** **IT Manager**	**CEO** **CFO**

• Notification from a software vendor, cloud service provider, internet service provider, or other technology supplier. *• Reports from staff, students, parents, governors, contractors, or other stakeholders.* *• Information received from external organisations, law enforcement agencies, the Department for Education, or the National Cyber Security Centre.* *• Reports received from third parties or members of the public.* *• Information reported through news outlets, media sources, social media platforms, or other public channels.*		
19.7 Delays in reporting cyber security incidents may increase the impact of an attack or data breach. All users are therefore expected to report concerns immediately, even where there is uncertainty as to whether an incident has occurred.	**School**	**CFO**
19.8 No individual will be criticised for reporting a suspected cyber security incident in good faith. The Trust encourages a culture of prompt reporting to minimise risk and protect its staff, students, and data.	**School**	

20.0 Response Plan Outline

	Responsible Body - School	**Responsible Body - Trust**
20.1 When a cyber security incident occurs, timely and coordinated action is critical to minimise disruption, protect Trust data, and reduce the impact on staff, students, and school operations. The response process shall be structured to support the rapid identification, containment, investigation, recovery, and review of the incident.	**IT Manager** **SLT**	**CEO** **CFO**
20.2 The Trust's communication systems, including email, telephony, and network services, may be unavailable or compromised during a significant cyber security incident. The Senior Leadership Team shall determine and direct the use of primary and alternative communication methods, including externally hosted services or emergency communication channels where necessary.	**SLT**	**CEO** **CFO**
20.3 Accurate information recording is essential throughout the lifecycle of an incident. The IT Department shall maintain a detailed chronological record of actions taken, systems affected, findings, decisions made, and communications issued. These records shall support incident management, lessons learned activities, regulatory requirements, and any subsequent legal or disciplinary proceedings.	**IT Manager** **IT Department**	**IT Manager**
20.4 Roles and responsibilities shall be clearly defined during an incident to ensure effective decision-making, communication, and coordination between the IT Department, Senior Leadership Team, Data Protection Officer, and any relevant external parties.	**SLT** **DPO** **IT Manager**	**CEO** **CFO**

20.5 Incident response activities shall prioritise the safety of pupils and staff, the protection of personal and confidential data, the continuity of educational operations, and the restoration of critical systems and services.	**SLT**	**CEO** **CFO**
20.6 Where appropriate, immediate containment measures shall be implemented to prevent further compromise, including isolating affected devices, disabling accounts, blocking malicious activity, or restricting access to affected systems.	**IT Manager**	**IT Manager**
20.7 Incidents that involve personal data, safeguarding concerns, significant operational disruption, or legal and regulatory obligations shall be escalated immediately to the appropriate members of the Senior Leadership Team and the Data Protection Officer.	**SLT** **DPO** **IT Manager**	**IT Manager**
20.8 Following resolution of an incident, the Trust shall conduct a post-incident review to identify lessons learned, assess the effectiveness of the response, and implement any improvements required to reduce the likelihood and impact of future incidents. Local Governing Bodies shall be informed	**LGBs** **SLT**	**CEO**

21.0 Response Plan Details

	Responsible Body - School	**Responsible Body - Trust**
21.1 All suspected cyber security incidents must be reported immediately to the IT Department. The method of detection will vary depending on the nature of the incident. For example, the loss or theft of a device may be identified through a report from a member of staff, whilst a cyber attack may be detected through system monitoring, security alerts, antivirus software, or reports from third-party suppliers.	**IT Manager**	**CFO**
21.2 Upon notification of an incident, the IT Department shall conduct an initial assessment to determine whether a genuine cyber security incident has occurred and assess its potential impact. Where appropriate, immediate action shall be taken to minimise risk and prevent further compromise.	**IT Manager**	**IT Manager**
21.3 Where an incident cannot be resolved through standard operational procedures or presents a significant risk to the Trust, its users, or its data, the IT Manager shall immediately notify the Senior Leadership Team, Chief Executive Officer, and Chair of Governors as appropriate.	**IT Manager** **SLT** **LGBs**	**CEO** **CFO**
21.4 The IT Department shall investigate the incident to determine: • *The nature and cause of the incident.* • *The systems, devices, accounts, or data affected.* • *Whether the threat remains active or has been contained.* • *The potential impact on Trust operations, safeguarding, and data protection obligations.* • *Any immediate actions required to support recovery.*	**IT Manager**	

All actions, decisions, findings, and timelines shall be recorded on the Incident Recovery Event Recording Form. *(See Appendix B).*		
21.5 Incidents shall be categorised according to their severity: • *Low: Minimal impact with no sensitive data involved and little or no disruption to services.* • *Medium: Limited exposure of sensitive information and/or disruption to one or more services.* • *High: Significant compromise of systems or sensitive data, major operational disruption, or prolonged loss of service.* • *Severe: Widespread compromise of Trust systems, significant data breach, ransomware event, or complete loss of critical services.*	**IT Manager**	**IT Manager**
21.6 Where specialist support is required, the IT Department shall escalate the incident to approved third-party IT providers, and any other relevant technical partners.	**IT Manager**	**IT Manager**
21.7 The IT Manager, in consultation with the Senior Leadership Team and Data Protection Officer, shall determine whether notification to external organisations is required, including the National Cyber Security Centre (NCSC), the Information Commissioner's Office (ICO), law enforcement agencies, insurers, the local authority, or other relevant bodies.(See ESCAT GDPR Policy	**SLT** **DPO** **IT Manager**	**CEO** **CFO**
21.8 The IT Department shall implement appropriate containment measures to prevent further damage. These may include isolating affected devices, disabling user accounts, blocking malicious network traffic, resetting passwords, restricting access to systems, or temporarily disconnecting services.	**IT Manager** **IT Department**	**IT Manager**
21.9 Where possible, evidence relating to the incident shall be preserved to support forensic investigation, regulatory reporting, insurance claims, disciplinary action, or criminal proceedings.	**SLT**	**CFO**
21.10 Once the threat has been contained, the IT Department shall coordinate recovery activities, including system restoration, account recovery, validation of backups, security testing, and the safe return of services to normal operation.	**IT Manager**	**CEO** **CFO**
21.11 The Senior Leadership Team working with the Local Governing Body shall determine whether it is safe and appropriate for the school to remain operational during the incident. Consideration shall be given to safeguarding, teaching and learning, examinations, communications, and business continuity requirements.	**SLT** **LGB**	**CEO** **CFO**
21.12 The Senior Leadership Team shall oversee communications relating to the incident and determine what information should be shared with staff, governors, parents, pupils, regulators, suppliers, and other stakeholders.	**SLT**	

21.13 Following restoration of services, a post-incident review shall be conducted by the IT Manager and Senior Leadership Team. The review shall identify lessons learned, evaluate the effectiveness of the response, and recommend improvements to systems, processes, training, or controls to reduce the likelihood and impact of future incidents.	**SLT** **IT Manager**	

.

Appendix A

Section		Page	Link
1.1	UK Data Protection and GDPR Act 2018	Page 3	Data protection: The UK's data protection legislation - GOV.UK
1.1	Keeping Children Safe in Education (KCSIE) 2025	Page 3	Keeping children safe in education - GOV.UK
3.1	Password Policy – DFE Guideline	Page 3	Meeting digital and technology standards in schools and colleges - Cyber security: core standard - Guidance - GOV.UK
3.1	Police Cyber Alarm	Page 4	Police CyberAlarm | Free Cyber Threat Detection Tool
3.1	NCSC Early Warning reporting	Page 4	NCSC Early Warning
9.0	Information Commissioner's Office	Page 9	Information Commissioner's Office

Appendix B

Incident Recovery Event Recording Form

Key Contacts – schools to add details as appropriate

Role in School	Name	Contact Details
Chief Executive Officer	Matthew Quinn	
Executive Head of School		
Head of School		
Headteacher		
IT Manager		
Chief Financial Officer / School Business Manager		
Data Protection Officer		
Site Mobile		
Facilities Manager		

Incident Recovery Event Recording Form

Description or reference of incident:	
Date of the incident:	
Date of the incident report:	
Date/time incident recovery commenced:	
Date recovery work was completed:	
Was full recovery achieved?	

Relevant Referral

Referral To	Contact Details	Contacted On (Time / Date)	Contacted By	Response

Action Log

Recovery Tasks (*In order of completion)*	Person Responsible	Completion Date		Comments	Outcome
		Estimated	Actual		
1.					
2.					

3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Post Incident Evaluation

Response Grades 1-5
1 = Poor, ineffective and slow / 5 = Efficient, well communicated and effective.

Action	Response Grading	Comments for Improvements / Amendments
Initial incident notification		
Enactment of the action plan		
Coordination of the Cyber Recovery Team		
Communications strategy		
Impact minimisation		
Backup and restore processes		
Were contingency plans sufficient?		
Staff roles assigned and carried out correctly?		
Timescale for resolution / restore		
Was full recovery achieved? If not, why not?		
What are the lessons learned from this incident?		
Log any requirements for additional training and suggested changes to policy / procedure:		