LDBS Academies Trust

LDBS Academies Trust
&
LDBS Academies Trust 2

Cybersecurity Policy

DATE APPROVED BY THE LDBS ACADEMIES TRUST	21st May 2025		
NEXT REVIEW DATE (Biennial)	May 2027		
SIGNED HEADTEACHER	Lisa Miles	DATE	05/05/2025
SIGNED CHAIR OF THE LOCAL ACADEMY COMMITTEE	Jenette Charles	DATE	05/05/2025

LDBS Academies Trust

Vision Statement

Our schools aspire to provide 'excellence and equity in a Christian context', where every child is valued as a unique individual treasured by a loving God.

'I have inscribed you on the palms of my hands.' Isaiah 49.v16.

Our aim is that every child will have the opportunity to flourish and develop into a rounded adult who can live life to the full.

'I have come that they may have life and may have it in all its fullness'. John 10.v10.

Our schools are places where all are welcome and where we practise kindness and hospitality on a daily basis. Our vision and our values are clearly displayed and while it is not a requirement that a child and their family have to be practising Christians, we do expect all parts of the community, children, staff, parents and carers to support the values that we hold dear.

In our school we demonstrate how we support this vision through our values which are — justice, trust, humility, reverence, peace, thankfulness, endurance, wisdom, creation, service, koinonia, friendship, forgiveness, compassion and hope.

We live out our values and vision through our key policies e.g. The behaviour policy is supported through the values described in the rewards and sanctions section of the policy demonstrating the importance of dignity and forgiveness.

The school admissions policy decided by the Local Academy Committee shows our inclusivity and the importance we place on service to our local community.

The breadth of the curriculum and the creative projects which we enjoy are key to providing opportunities for children to experience life in 'all its fullness', so that alongside learning and wisdom they also experience joy and delight in learning.

Care for the individual and their needs is crucial and the school's policies regarding inclusion and SEND are constant reminders that each of us is known to God and our names are 'inscribed on the palms of His hands'.

The HR policies are common in all Trust schools and are created to ensure that individuals are treated fairly and with dignity. All HR policies have been scrutinised by the various unions to ensure that they contain acceptable procedures.

LDBS Academies Trust

Contents

Introduction....3

Scope of Policy....4

Risk Management....4

Physical Security....4

Asset Management....4

User Accounts....4

Devices....5

Data Security....5

Sharing Files....5

Training....6

System Security....6

APPENDIX I....6

Introduction....7

Definitions....7

Purpose of Plan....7

IRP Ownership....7

Incident Response Team....7

IRT Contact Details....8

IRT Communications....8

Key Documents and Files....8

Recovery Priorities....9

Key Service Providers....10

Incident Plan....11

Response Plan....11

Actions Log....12

Review and sign off....13

Introduction

This policy has been created in partnership with London Grid for Learning (LGFL).

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents (Please refer to Appendix I) such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cybersecurity Policy outlines Holy Trinity's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Scope of Policy

This policy applies to all Holy Trinity's staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Risk Management

Holy Trinity's will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Governors 2 times a year.

Physical Security

Holy Trinity will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Holy Trinity will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform Cringe, our IT support, as soon as possible. Personal accounts should not be used for work purposes. Holy Trinity will implement multi-factor authentication where it is practicable.

Devices

To ensure the security of all issued devices and data, users are required to:

Lock devices that are left unattended
Update devices when prompted
Report lost or stolen equipment as soon as possible to Cringe
Change all account passwords at once when a device is lost or stolen (and report immediately to Cringe)

Report a suspected threat or security weakness in Holy Trinity's systems to Cringe and the DPO.

Devices will be configured with the following security controls as a minimum:

Password protection
Full disk encryption
Client firewalls
Anti-virus / malware
software Automatic security
updates
Removal of unrequired and unsupported
software Autorun disabled
Minimal administrative accounts

Data Security

Holy Trinity will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Holy Trinity's defines confidential data as:

Personally identifiable information as defined by the ICO Special Category personal data as defined by the ICO
Unpublished financial information
Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology
3 versions of data
2 different types of media
1 copy offsite/offline

Sharing Files

Holy Trinity recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date breach users are required to:

Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
Wherever possible, keeping Holy Trinity's files on school systems Not sending school files to personal accounts
Verifying the recipient of data prior to sending

Using file encryption where possible, sending passwords/keys via alternative communication channels
Alerting [IT Support/DPO] to any breaches, malicious activity or suspected scams

Training

Holy Trinity recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

System Security

Cringe will build security principles into the design of IT services for Holy Trinity CE Primary School.

Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems Segregate wireless networks used for visitors' & staff personal devices from school
- systems

Review the security risk of new systems or projects

APPENDIX I

MAJOR INCIDENT RESPONSE PLAN

Introduction

This is an IT major incident response plan for Holy Trinity CE Primary School. This plan is to be invoked in the event of an incident that would affect IT services for the school.

Definitions

Incident Response Plan (IRP)

A documented set of procedures and information intended to deliver continuity of critical IT activities in the event of a disruption.

Incident

An event that causes disruption to the organisation.

Critical IT services could be disrupted by loss of:

key data because of a ransomware attack

key services because of a ransomware

attack communications networks (e.g.

email, phones) other key services (e.g.

school MIS).

Purpose of Plan

The purpose of this plan is to minimise the impact of such losses by making contingency plans and putting measures in place for essential IT processes to be maintained.

IRP Ownership

Lisa Miles has overall responsibility for the IRP and has delegated responsibility for documenting the process to Elliott Bergin, School Business Manager.

The IRP will be reviewed and updated every year, or when other factors dictate. Updated plans will be signed off by Lisa Miles and circulated to replace the previous versions.

Incident Response Team

In the event of a major incident an Incident Response Team (IRT) will be formed. The key roles of the
IRT are to:

Make decisions to apply appropriate
resources Provide strategic direction
Provide communications to key internal and external stakeholders (staff, students, parents, public bodies)
Assume responsibility for co-ordinating incident
management Liaise with Third party suppliers

If possible, it can be useful to include a Governor and a member of staff who is not technically aware in this group to get a variety of perspectives

IRT Contact Details

Name	Contact Details
Lisa Miles, Headteacher	office@ht309.ldbsact.org 0208 808 2588
Ben Hobbis, Assistant Headteacher	office@ht309.ldbsact.org 0208 808 2588
Elliott Bergin, School Business Manager	office@ht309.ldbsact.org 0208 808 2588
Cringe, IT Support	Through the helpdesk and via telephone

IRT Communications

This section should be completed to detail how the IRT will communicate with each other and key stakeholders during a Major Incident. It should be assumed that access to email, telephones and websites could be affected by the incident. Alternative methods should be tested and documented, including details of where backup contact information can be accessed. It may be necessary to print contact lists or store them on offline media.

Key Documents and Files

This table should be completed to detail the location of documents that may be required during a major incident

Document of File Name	Location	Backup Location	Document Owner
Major Incident Response Plan	School Office (locked cabinet)	On Teams Channel	Headteacher & School Business Manager

Staff contacts list	School Office (locked cabinet)	Arbor & Personnel Files	School Business Manager
Parents contacts list	School Office (locked cabinet)	Arbor & Personnel Files	School Office Team
Third party contacts list	School Office (locked cabinet)	On Teams Channel	School Business Manager
Insurance documents	School Office	On Teams Channel	School Business Manager
Network documentation	Major Incident Response Plan Folder	On Teams Channel	Cringe IT support
Secure password repository	Cringe IT Support Secure Password Vault	Encrypted Backup Repository	Cringe IT Support
Backup disk/media recovery keys	Cringe IT Support Secure Storage	Encrypted Offline Storage	Cringe IT Support

Recovery Priorities

This section details the order in which systems should be restored to ensure that critical functions are available as soon as possible. As different systems have different priorities throughout the year this order should be reviewed by the IRT to ensure that it is still appropriate. For instance, the restoration of the school's MIS may be a higher priority during exam results weeks.

System/Service	Pre-requisites	Priority	Notes
Backup solution	None	Very High	Required for all recovery activities
Active Directory/User account administration	Backup solution	Very High	Required for the majority of other services
Office 365/ Google Workspace Email/OneDrive/G Drive	Active Directory (depending on configuration)	Very High	Primary Communication Tools
Management Information System	Active Directory	High	Attendance, Safeguarding & Pupil information

Phone system	None	High	Not integrated to other systems
User files	Active Directory	Medium	
Access control	None		Not integrated to other systems
CCTV	None	Medium	Not integrated to other systems
Education Apps	Active Directory	Low	Not essential to immediate operations
Printing	Active Directory	Low	Alternative manual processes possible
Cashless catering	Internet Access	Low	Alternative manual catering procedures available
Safeguarding Systems (CPOMS)	Active Directory / Internet	Very High	Critical safeguarding records
SEND Records	Active Directory / Arbor	Very High	Essential pupil support information
Printing	Active Directory	Low	Alternative manual processes possible

Key Service Providers

This section provides a record of key service providers that form part of the school's IT services.

Name	Type/Description of Service	Contact Details
Police - Action Fraud	National reporting centre for fraud and cybercrime	0300 123 2040
Haringey Council / LDBS Academies Trust	Strategic support and incident escalation	Existing LA and Trust contacts
Information Commissioner's Office (ICO)	Data Protection Regulator	ico.org.uk / 0303 123 1113
BT	Telephone Services	Through BT Business Support
Sophos	Antivirus and endpoint protection	Sophos Central Portal
Malwarebytes	Anti-malware protection	Malwarebytes Portal
Gridstore	Cloud Backup Solution	Gridstore Support Portal
Cringe IT Support	Managed IT Support	Existing Support Agreement
Stone Computers (or existing supplier)	Hardware Supplier	Supplier records
Microsoft	Office 365 Licensing	Microsoft 365 Admin Portal
WJ Fire	CCTV Maintenance Provider	Supplier records
Paxton (or existing provider)	Access Control Provider	Supplier records
Commissioner's Office	charge of upholding information rights – inform	Website 0303 123 1113

	within 72 hours if data is stolen during the incident.	

Incident Plan

Response Plan

Risk	Potential Triggers of the risk	Current mitigations
Loss of access to files and IT Systems	Ransomware attack Sabotage Phishing emails Fire/Flood Pandemic DDoS (Distributed denial of Server) Power failure	Daily backups encrypted and stored offsite Staff have remote access to email Files and folders stored on Microsoft Office 365 systems Antivirus software installed on all systems and checked regularly for correct configuration and automatic updates running Security updates applied to devices as soon as possible Administrative permissions limited to IT support staff Sophos phish used to raise awareness of threats

1. Actions required in the event of a major incident

	Action	Timing	Responsible	Complete
1.1	Verbal notification of incident / or identifies a problem through system alerts	Immediate	Cringe	
1.2	Notification to IRT	Immediate	Cringe	

1.3	Assessment of scope of incident and options for limiting impact	Within 1 Hour	Cringe	
1.4	Review recovery priorities	Within 1 Hour	IRT	
1.5	Communicate with school staff Inform Action Fraud	Within 1 Hour	IRT	
1.6	Estimated recovery time / invoke full or partial recovery plan	Within 1 Hour	IRT	
1.7	Communicate with parents if required as part of school day	Within 2 Hours	Lisa Miles	
1.8	Regular updates to IRT and school staff	2 Hourly	Lisa Miles	
1.9	Communicate with Public bodies as required	As required	Lisa Miles	

Actions Log

During a Major Incident a lot of things can happen very quickly. Good record keeping can help save time in the future. The following table should be used to track what has been done and by whom.

Following the incident this can be used to review the effectiveness of this plan and the actions that were undertaken.

Date	Time	Description of the event/ action taken/ decision made	Costs incurred	Completed by

LDBS Academies Trust

Review and sign off

HOLY TRINITY CE Primary School	Headteacher	Lisa Miles
	School Business Manager	Elliott Bergin
	Network manager / other technical support	Cringe
	Date this plan was last reviewed and by whom	05/05/2026
	Date of next review and by whom	05/05/2027