DIOCESE OF

ST ALBANS

MULTI-ACADEMY TRUST

Trust Cybersecurity Policy

Policy type	Trust wide (Tier 1)
Reviewal timeframe	Annually
Author/Responsible Officer	Gov professional, PEL and DPO (Handsam)
Board to be ratified	Audit, Risk and Compliance
Approved by	Head of Governance
Date of ratification	September 2025
Date of next review	September 2026

This policy is a mandatory policy for all DSAMAT Academies and must be implemented without any amendments

Enabling all to flourish: Rooted in God's love

Our mission, vision and values

The Trust has a clear **mission** at its core, ensuring that all pupils are enabled to flourish, rooted in God's Love - academically, socially, spiritually, physically and mentally. This is central to our work and rooted in our Christian foundation (John 10 v 10). Our commitment to mutual flourishing within the school community is built upon our shared belief in Church of England principles. In our Trust, just as in the wider Church of England community, 'flourish' refers to prospering, thriving and growing – not shrinking out and dying. It means prayerfully encouraging all within our schools so that they might prove fruitful, successful and contented in the longer term. We seek to provide space generously for all to flourish in life and all of its structures. Equal treatment for all pupils, staff and the wider community is a core part of enabling this long term, holistic flourishing.

We have a clear **vision** about creating successful schools for the benefit of their communities and we expect every school in the Trust to continuously improve. All schools provide rich and diverse curricula which evolve to meet the needs of their children and local communities, as well as delivering educational excellence to enable them to continue to flourish in later life.

The way we work and deliver against our mission is critical to our Trust. We have shared, agreed **values** of:

Hope; Nurture; Equality; Respect; Collaboration

The Trust's vision is underpinned by a Christian values framework which is adopted by all schools. It provides clear expectations for all Trust employees on how we wish our values to impact on all areas of school life. It draws on, and is informed by, the National Church of England Vision for Education and the Diocesan Board of Education Vision.

Each school within the Trust has a personalised vision for education, developed locally to reflect the individual character and needs of the school community. This vision is underpinned by the Trust's wider vision, and agreed with the Trust, but it is owned and driven by the headteacher and their LGB.

Our community

The Trust are dedicated to delivering education that serves local communities. Our schools are inclusive, welcoming those from all and no faiths, from all abilities and backgrounds. We believe in providing a high-quality education, underpinned by Christian values, which enables every child to flourish.

Underpinning all of the Trust's work is a belief in educational excellence. The Trust serves all stakeholders by providing schools with the highest levels of academic rigour and pastoral care.

Our schools are places where children and young people develop and thrive intellectually, socially, culturally and spiritually. All of the Trust's schools teach a broad and balanced curriculum within national guidelines focusing on core skills. This is designed to ensure that all pupils reach their academic potential and seek to enrich their experience along the way. Pupils will be enabled to succeed in an atmosphere of high expectation, aspiring to educational excellence with a firm foundation of values.

This policy forms part of our Trust governance and ensures that we are held to the highest standards as we carry out our duties.

Statement of Intent

This is the Diocese of St Albans Multi-Academy Trust (DSAMAT) over-arching Cybersecurity policy and must be implemented and adhered to in each of the academies within the Diocese of St Albans Multi Academy Trust along with those working within the central team.

This policy will also be implemented and adhered to from the first day of any other academy joining the Trust.

For the remainder of this document, the Diocese of St Albans Multi Academy Trust will be referred to as DSAMAT.

Contents

1. INTRODUCTION

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 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 DSAMAT's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Our Academies:

- Caldecote Church of England Academy
- Churchfield Church of England Academy
- Great Barford CE Primary Academy
- Kensworth Church of England Academy
- Manshead Church of England Academy
- Northill CE Academy
- Ravensden CofE Primary Academy
- Roxton Church of England Academy
- St James' CE Academy
- St Leonard's Church of England Academy
- Studham Village CE Academy
- Thomas Whitehead Church of England Academy
- Totternhoe Church of England Academy
- Ursula Taylor Church of England School
- Wenlock CE Academy

2. ROLES AND RESPONSIBILITIES

It is the responsibility of the DSAMAT Data Controller to:

- Oversee the adherence to data protection law and the safety of processing activities on site;
- Ensure that safe and confidential systems are in place across the trust and consult the Data Protection Manager in DSAMAT Academies in the implementation, development and monitoring of data processing activities;
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented to the personal data processed; and
- Provide information to bodies entitled to receive information under data protection law.

It is the responsibility of each member of staff to adhere to this policy, standards and procedures. It is the school's responsibility to ensure the security of their information, ICT assets and data. All members of the central team and school community have a role to play in information security.

3. RISK MANAGEMENT

The central team and each academy will, in collaboration with Partnership Education and their IT technician, identify and assess the potential cybersecurity risks for their organisation. These will be collated trust wide and evidenced on the DSAMAT Risk Register.

4. PHYSICAL SECURITY

Each academy 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.

5. ASSET MANAGEMENT

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

6. USER ACCOUNTS

Users are responsible for the security of their own accounts as detailed in the Acceptable Use Agreements. 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 a member of IT Support as soon as possible. Personal accounts should not be used for work purposes. Each academy will implement multi-factor authentication where it is practicable to do so.

7. DEVICES

To ensure the security of all Trust / academy 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 their line manager and a member of IT Support
- Change all account passwords at once when a device is lost or stolen (and report immediately to a member of IT Support)
- Report a suspected threat or security weakness in the academy's systems to Headteacher or member of the senior leadership team.

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

All DSAMAT staff, Directors, governors and volunteers are expected to sign and adhere to the ICT Acceptable Use Policy.

The Data Protection Manager and Data Controller will ensure that all staff are aware of the dangers of taking data off the school's immediate environment and are aware of the procedures in place to minimise the risk.

All devices storing data such as laptops and any work phones must be password protected, and data encrypted. Staff will not remove any more data than is necessary from the premises and will consult the Data Protection Manager regarding the specific data movement requirements of their role.

8. CLOUD MANAGEMENT

Where possible, DSAMAT will utilise cloud based management systems for operational purposes. In doing so the following steps will be taken:

- All cloud based systems will go through a DPIA approval process prior to being used.
- Each school will use Arbor as their cloud based management information system.
- Office 365 will be the cloud based business system used across all DSAMAT users.
- MFA will deployed wherever possible.
- Guidance will be provided for users on what data should and should not be kept on each system, in line with our Data Protection Policy.
- Access to DSAMAT cloud based systems should be on DSAMAT devices, unless special permission to use a personal device has been given by the Headteacher / central executives.

9. DATA SECURITY

Each academy and the central team will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential and critical data and critical systems. The DfE Indicators for potential fraud: a generic checklist for education providers will be utilised to facilitate a comprehensive approach.

Confidential data is defined 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 on the Trust wide Redstor cloud back-up solution, with clear specification as to what should be backed up to this system for each school and the central services.

10. SHARING FILES

DSAMAT 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 files on school / centralised systems
- Not sending 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 a member of IT Support and DPO to any breaches, malicious activity or suspected scams

11. TRAINING

DSAMAT recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. The Trust will share and ask all members of staff to complete the National Cyber Security Training annually (Cyber security training for school staff - NCSC.GOV.UK) with each school maintaining their own record of completion.

Regular Cybersecurity reminders and updates will be shared Trust wide via Weekly Operations Updates. We will promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

12. SYSTEM SECURITY

IT Support will build security principles into the design of IT services for the central team and each academy including:

- Security patching – network hardware, operating systems and software
- Pro-actively planning 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
- Review the security risk of new systems or projects

DSAMAT and its academies will ensure that once a specified data retention period has passed that all such data is safely destroyed. Processes shall include:

- For physical documents: Shredding
- For digital data: Wiping with confirmation statement/certificate to be held in perpetuity

- For disposal of IT equipment of any kind: Use of an accredited specialist provider with confirmation statement/certificate to be held in perpetuity

The Data Manager / Data Controller shall take charge of ensuring that all aspects of data across all areas of the organisation are considered for this process once per term (i.e. three times per year).

13. BUSINESS CONTINUITY PLAN

The central team and each academy will develop, maintain, and regularly test a Business Continuity Plan. This will include identifying or carrying out:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)

14. MAINTAINING SECURITY

DSAMAT understands that the financial cost of recovering from a major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems.

In order to proactively budget appropriately to keep cyber related risk to a minimum the following steps will be taken:

- Maintain an effective refresh cycle for all IT equipment (devices and infrastructure) to ensure that hardware is replaced before it goes "end of life" and stops receiving security updates from the manufacturer.
- PEL will support the schools in providing recommended 3-5 year budgets and highlighting any relevant end of life notices that affect current equipment
- Allocate budget, where advised, to dedicated security tools or support which come out of the Trust cyber assessments and security planning. These will continually be under review and subject to change but may include cloud backup, training resources, phishing simulation tools, penetration testing or other dedicated security systems

15. MONITORING AND REVIEW

This policy will be reviewed annually and approved by a member of the Central Trust SLT