STOUR VALE ACADEMY TRUST

INFORMATION AND CYBER SECURITY POLICY

VERSION / DATE	VERSION 6.3 MARCH 2024
NEXT VERSION DUE BY	MARCH 2027

Contents

Information and Cyber Security Policy for Stour Vale Academy Trust

Policy Statement

Stour Vale Academy Trust ('the Trust'), comprising the member schools and central team, will ensure the protection of all information assets within its custody.

High standards of confidentiality, quality and availability of information will be maintained at all times.

The Trust will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of an information and cyber security policy, including the supporting guidance documents which are listed below.

Purpose

Information is a major asset that the Trust has a responsibility and requirement to protect. The secure running of the Trust is dependent on information being held safely and securely.

Information used by the Trust exists in many forms, and this policy includes the protection of information stored electronically, transmitted across networks and printed or written on paper. It also includes any information assets in Cyberspace (the cloud). UK Cyber Security Strategy 2011 defined Cyberspace as:

'Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.'

Protecting personal information is a legal requirement under Data Protection Law.

The Trust must ensure that it can provide appropriate assurances to its pupils, parents and staff about the way that it looks after information ensuring that their privacy is protected and their personal information is handled professionally.

Protecting information assets is not simply limited to covering the information (electronic data or paper records) that the Trust maintains. It also addresses who has access to that information, the processes they follow and the physical computer equipment used to access them.

This Information and Cyber Security Policy and associated guidance documents, as listed below, address all of these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets.

Scope of the Policy

This Information and Cyber Security Policy and associated guidance documents, as listed below, apply to all systems, people and school processes that make up the Trust's information systems. This includes all members and trustees, governors, staff and agents of the Trust who have access to Information Systems or information used for Trust purposes.

Definition

This policy should be applied whenever Trust information systems or information is used.

Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper
- Data stored electronically (on site, on a network or in the cloud)
- Communications sent by post / courier or using electronic means
- Stored tape or video
- Speech

Risks

The Trust recognises that there are risks associated with users accessing and handling information in order to conduct official Trust business.

The Trust is committed to maintaining and improving information security and minimising its exposure to risks. It is the policy of the Trust to use all reasonable, practical and cost-effective measures to ensure that:

- information will be protected against unauthorised access and disclosure;
- the confidentiality of information will be assured;
- the integrity and quality of information will be maintained;
- authorised staff, when required, will have access to relevant Trust systems and information;
- business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained;
- access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/documented agreements;
- all breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken;

- information security training will be available to all staff;
- regular review of Information and Cyber Security Policy and associated guidance documents, as listed below, will be carried out;
- this policy will be reviewed when significant changes affecting the Trust are introduced;
- an Information Security framework of policies and guidance will be developed and implemented consistent with this policy;
- the school's Information and Cyber Security arrangements will be subject to review by the Senior Information Risk Owner (SIRO) supported by the Trust's Data Protection Officer.

Non-compliance with this policy could have a significant effect on the efficient operation of the Trust and may result in financial loss and embarrassment.

Roles and Responsibilities

It is the responsibility of each member of staff to adhere to this policy, standards and procedures. It is the Trust's responsibility to ensure the security of their information, ICT assets and data. **All** members of the Trust community have a role to play in information and cyber security. Refer to Appendix 1 for information on the role of the Senior Information Risk Owner (SIRO), Data Protection Officer (DPO) and Information Asset Owners (IAO).

Supporting guidance documents

The Trust should refer to guidance documents that are directly relevant to this policy. These include the Trust data protection policy, school information asset registers, security incident reporting guidance and CCTV policies. Reference may also be made to relevant guidance issued by external ICT providers used by the Trust.

Version Control

This policy will be evaluated every three years or more frequently as required.

Further information

For further information, please contact:

YourIG Data Protection Officer Service
Dudley MBC, The Council House, Dudley, West Midlands, DY1 1HF

Email: YourIGDPOService@dudley.gov.uk Tel: 01384 815607

Appendix 1 Roles and Responsibilities

Role of the Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff within the Trust who is familiar with information risks and the Trust's response. Typically, the SIRO should be the Chief Executive Officer, Headteacher or a member of the Senior Leadership Team and have the following responsibilities:

- own and maintain the Information Security Policy
- establish standards, procedures and provide advice on their implementation
- act as an advocate for information risk management
- appoint the Information Asset Owners (IAOs)

Additionally, the SIRO will be responsible for ensuring that:

Staff receive appropriate training and guidance to promote the proper use of information and ICT systems. Staff will also be given adequate information on the policies, procedures and facilities to help safeguard the Trust's information. A record of the training provided to each individual member of staff will be maintained.

Staff are made aware of the value and importance of Trust information, particularly information of a confidential or sensitive nature, and their personal responsibilities for information security.

The associated guidance relating to information security and the use of particular facilities and techniques to protect systems and information, will be disseminated to staff.

The practical aspects of ICT protection are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

There are appropriate controls over access to ICT equipment and systems and their use, including defining and recording the requisite level of protection.

They are the official point of contact for ICT or information security issues and as such have responsibility for notifying the Executive Team, Senior Leadership Team, Data Protection Officer, Chair of Trustees and Chair of Governors of any suspected or actual breach occurring within the Trust.

The Trust's Senior Information Risk Officers (SIRO) are the Headteachers for each member school and the Chief Executive Officer for the central and executive team.

Role of the Data Protection Officer (DPO)

Article 37 of the UK General Data Protection Regulation (UK GDPR) mandates that schools and academies have a Data Protection Officer (DPO) in place.

The role of the DPO within the Trust is to:

- advise the Trust, their data processors and their employees of their responsibilities;
- monitor the Trust's compliance with UK GDPR and other data protection legislation and internal policies;
- advise on data protection impact assessments;
- monitor performance;
- identify safeguards to apply to mitigate any risks identified;
- maintain a record of processing activities;
- maintain records and evidence of the Trust's compliance with the UK GDPR;
- conduct audits to ensure compliance and address potential issues (including an annual benchmark audit).

The DPO will also be the contact point for the Information Commissioner's Office (ICO).

The Trust's Data Protection Officer is:

YourIG Data Protection Officer, Dudley MBC, The Council House, Dudley, DY1 1HF
Email: YourIGDPOService@dudley.gov.uk Tel: 01384 815607

Role of the Information Asset Owner (IAO)

Once the Trust has identified its information assets, including personal information and data relating to pupils and staff, for example, assessment records, medical information and special educational needs data, the Trust should identify an Information Asset Owner (IAO) for each asset or group of assets as appropriate.

The role of an IAO is to understand:

- what information is held and for what purposes;
- how information will be amended or added to over time;
- who has access to the data and why;
- how information is retained and disposed of.

Typically, there may be several IAOs within a Trust, for example, Business Manager, ICT Manager.

The IAO is responsible for managing and addressing risks to the information and ensuring that information handling both complies with legal requirements and is used to fully support the delivery of education.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records e.g. archives
- Computer databases
- Data files and folders

On the introduction of this policy, Information Asset Owners may need to conduct a thorough information risk assessment to identify any necessary operational or technological changes that may be required within the Trust.