Information Governance Policy 2024-25

Document Control	
Owning Function:	Data Protection Officer
Date Approved by Executive:	4 June 2024
Date Approved by F&A Committee:	2 October 2024
Next Revision Date:	Term 2 2026/27

Change History	
Date	**Description**
June 2024	Current Version

1. Summary

This Policy establishes the key high-level principles of Information Governance at the University of Chichester Academy Trust ('the Trust') and sets out responsibilities and reporting lines for members of staff. It provides an over-arching framework for Information Governance across the Trust.

2. Scope

The Policy applies to Trustees, Governors, Staff, Contractors and Volunteers of the Trust and any organisation that holds or carries out work on behalf of the Trust. Reference to the Trust is reference to its academies.

3. Introduction

Information is generally defined as "knowledge or facts about someone or something" and "the communication or reception of knowledge or intelligence". It can exist in many different formats, but it must have meaning in some context for its receiver.

Information governance is an accountability and decision-making framework put in place to ensure that the creation, storage, use, disclosure, archiving and destruction of information is handled in accordance with legal requirements and to maximise operational efficiency. It includes the processes, roles, policies and standards that ensure the compliant and effective use of information in enabling an organisation to achieve its goals.

Information is a key asset for the Trust and the regulatory, reputational and operational risks of poor information governance are ever increasing. As the creation of information proliferates, it is vital that the Trust has measures in place to manage and control these risks. The management and use of information is key to achieving the Trust's wider aims as set out in its Strategic Plan.

The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.

4. Roles and Responsibilities

There are a number of key roles and responsibilities across the Trust in relation to information governance, as set out below. The framework diagram at Appendix 1 details the relationships between the various roles:

4.1. Board of Trustees

The Board of Trustees has responsibility and accountability for ensuring strategic direction of the Trust and holding executive leaders to account for the educational performance of the organisation and its pupils. As such, will ensure the Trust has appropriate information governance procedures in place to mitigate risk and maximise the value of the information it holds.

4.2. Finance and Audit Committee

The Board established a Finance and Audit Committee that has responsibility for data protection, including the General Data Protection Regulation (GDPR). The Committee ensures the Trust has robust information governance and security processes and procedures in place. Colin James is the named Trustee lead for Data Protection.

4.3. Data Protection Officer (DPO)

The DPO is accountable at a senior management level for ensuring the Trust has robust information governance and security processes and procedures in place.

This role is also responsible for managing the Trust's Information Asset Register and compliance across the Trust with the Data Protection Act/General Data Protection Regulation, Freedom of

Information Act and other relevant legislation. This role holds the statutory Data Protection Officer role as designated by the Data Protection Regulation.

4.4. Local Governing Body Designated Data Protection Lead (DDPL)

All local governing bodies will appoint a Designated Data Protection Lead to hold the relevant academy to account to ensure compliance with legislative and Trust requirements in respect of handling, recording and storing of information, where potential risks are mitigated.

4.5. Data Champions (DC)

Data Champions are either members of the senior leadership team across the Trust, or who represent SLT and have responsibility for data protection within a specific function area or academy. Their role is to promote best practice and ensure compliance with data protection, ensuring information is handled and managed properly, that appropriate access and security controls are in place and that the accuracy and integrity of the information is assured and consistent. They provide assurance to the DPO that the information risk is being managed effectively and update the Information Asset Register they have responsibility for.

4.6. Data Information Asset Administrators (IAAs)

IAAs are members of staff that have been delegated responsibility for the operational use of information assets within a function area, academy or Partnership area. Their role is to process, identify and report any operational concerns or risks to the DC to be escalated accordingly.

4.7. IT Services

The Director of Finance or Academy Leader has operational responsibility for ensuring that the IT provider/s and their employees comply with information governance processes and procedures in place across the Trust. Furthermore, the IT provider/s have responsibility for ensuring robust and effective information security processes and procedures in place and that are approved by the Trust.

This role monitors the Trust's compliance with the Information Security Policy and handles information security incidents when they arise and reports any concerns to the Director of Finance, Academy Leader or DC to manage or escalate accordingly.

4.8. All staff, Trustees, Governors, Volunteers and third party contractors

All staff , including irregular and part-year workers, contractors, governors, trustees, volunteers or students who carry out work, whether paid or unpaid, on behalf of the trust, are responsible for ensuring that they are aware of the requirements of the Trust's policies in relation to information governance and security and adhere to them on a day to day basis.

All staff are responsible for highlighting areas of perceived risk where information practices could be improved and to report any incidents that could be considered a breach of the Trust's internal policies or external legislation. All staff will be required to enter into confidentiality obligations with the Trust and to participate in information governance training during induction and periodically throughout their employment or engagement. Any breach of confidentiality and/or the Trust's information governance and security policies may be a contractual and/or disciplinary matter which could result in termination of an individual's employment or engagement by the Trust.

5. Legal and compliance

The Trust's information governance framework must ensure compliance with various pieces of legislation relating to the handling and use of information, as well as the common law duty of confidentiality. These include, but are not limited to:

- Data Protection Act 2018
- General Data Protection Regulation (Regulation (EU) 2016/679
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Environmental Information Regulations 2004

- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) Regulations 2000
- Computer Misuse Act 1990
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Official Secrets Act 1989
- Malicious Communications Act 1988
- Digital Economy Act 2010
- Intellectual Property Act 2014
- Investigatory Powers Act 2016

6. Records and Document Management

The Freedom of Information Act Section 46 Code of Practice1 sets out a number of principles in relation to records management:

- Recognition of records management as a core corporate function;
- Inclusion of records and information management in the corporate risk management framework;
- A governance framework that includes defined roles and lines of responsibility;
- Clearly defined instructions, applying to staff at all levels of the authority, to create, keep and manage records;
- Identification of information and business systems that hold records and provision of the resources needed to maintain and protect the integrity of those systems and the information they contain;
- Consideration of records management issues when planning or implementing ICT systems, when extending staff access to new technologies and during re-structuring or major changes to the authority;
- Induction and other training to ensure that all staff are aware of the authority's records management policies, standards, procedures and guidelines and understand their personal responsibilities;
- An agreed programme for managing records;
- Provision of the financial and other resources required to achieve agreed objectives in the records management programme.

The Trust's Retention Policy and Retention and Destruction Guide sets out the consistent standards that staff should use when creating, using and disposing of information.

7. Training

The Trust will ensure relevant training is in place to assist staff in their day-to-day handling of information.

All new staff must complete data protection training, together with the NSCS Cyber Security training for RPA insurance purposes to ensure they are aware of the risks and their responsibilities in handling information. Staff will be required to complete refresher training annually reflecting any changes and updates in information governance best practice.

All Data Champions must complete additional training as determined by the Data Protection Officer.

All Trustees and Governors must complete data protection training and refresher training to ensure they are aware of their responsibilities in handling information and effectively and appropriately challenge to ensure compliance.

8. Interaction with other policies and procedures

The Trust has a number of policies and procedures that have relevance to information governance, as below, and staff must be aware of their content:

8.1. Information Governance Policies:

- Data Protection Policy
- Privacy Notice
- Retention and Deletion Policy
- Electronic Information Security Policy – Schools
- Freedom of Information Policy
- Photography Policy
- Critical Incident Plan of relevant academy

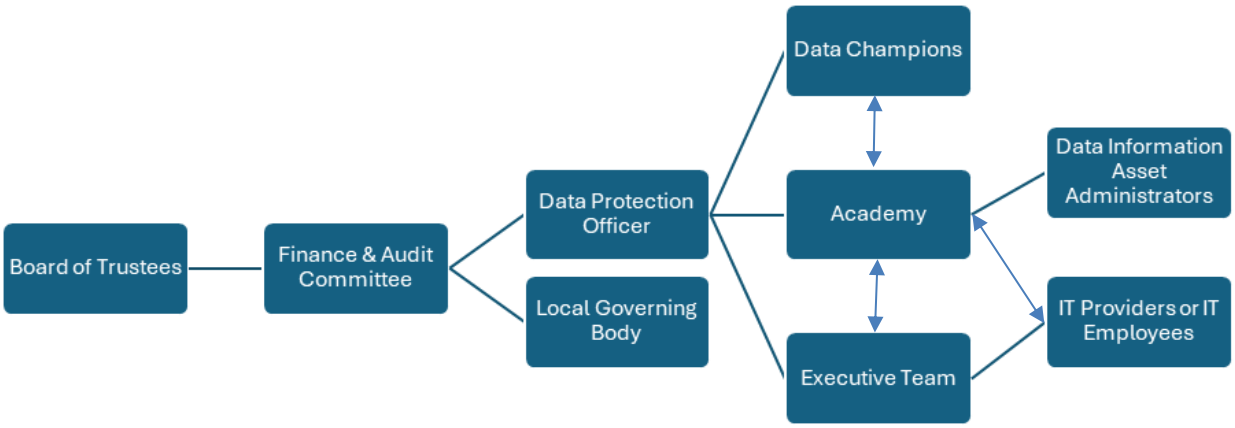
8.2. Other policies and guidance:

- GDPR Guidance for Academies
- Retention and Destruction Guidance
- Data Impact Assessment Guidance
- Multi-media consent forms
- Due Diligence for third party processors

9. Policy Review and Ownership

This policy will be reviewed as required and at least every three years by the Finance and Audit Committee. The document is managed by the Data Protection Officer in the central office.

-end-


Board of Trustees
Finance & Audit Committee
Data Protection Officer
Local Governing Body
Data Champions
Academy
Executive Team
Data Information Asset Administrators
IT Providers or IT Employees