Data Governance Policy

Contents

1.0 Policy statement

Data governance is an organisational approach to data and information management that is formalised as a set of policies and procedures that encompass the full life cycle of data; from acquisition, to use, to disposal.

Everyone has a responsibility to look after Trust data, and abide by Trust policy, and all applicable laws including the General Data Protection Regulations (GDPR). Data matters because it is essential to Trust processes and is used on a daily basis to make decisions. Everyone uses data in what they do (processes) and often this data is provided by (IT systems) technology. Mismanagement of data by students, staff or others may lead to fines, reputational damage, and can have other process and financial implications.

2.0 Scope and purpose

Information, in all its forms, is a primary resource of the Trust. Its effective curation and protection is critical to the effective running and reputation of the Trust.

The objective of the Data Governance Policy (the "Policy") and supporting Data Security is to protect the Trust by preventing and limiting the impact of information security problems that might damage the Trust's operation, reputation or business.

Benefits of applying this policy will include, ensuring data is fit for the purposes of internal and external reporting, and is appropriately categorised for storage, retrieval, destruction, backup, and access as needed to ensure proper management and protection of Trust Data. It will ensure that:

- decisions at all levels can be made based on trustworthy data and therefore lead to better decisions
- build standard, repeatable processes
- costs are reduced and effectiveness increased through coordination of processes
- regulatory requirements (such as GDPR) are met
- risk is reduced of the mismanagement of data for students, staff and others; which may lead to fines, reputational damage, and can have other process and financial implications
- data security is improved by establishing data ownership
- business continuity is maintained by ensuring the availability and disaster recovery of key data
- the IT strategy is supported in making key decisions
- there is greater accountability for data distribution
- data is stored, maintained and classified in the optimal way to be quickly accessible
- data meets the needs of each individual within the organisation to optimise agility

The Data Governance policy will clarify who can take what action, with what data and under which circumstances, using what methods.

3.0 Principles

3.1 Principles apply to all forms of data governance and planning, and guide governance decisions, process and systems development. Dixons Academies Trust shall ensure that an approved set of principles for data is reviewed, agreed and is compatible with other governance requirements. Data policies that impact general Information Security shall be reviewed and approved by the Executive alongside the Trust Board.

The current set of approved principles is summarised below:

- data is an Asset - Data is an asset that has value to the Trust and is managed accordingly. Look after data and protect it
- data that has shared value should be shared - Users have access to the data necessary to perform their duties; therefore, data is shared across Dixons Academies Trust and external organisations as appropriate. Use of data shall comply with the direction set by the Data Steward (e.g. people data shall be handled in accordance with the direction set by the people data steward, wherever that data is held in the Trust)
- data is Accessible - Data is accessible for users to perform their agreed functions when and how they need it
- common Vocabulary and Data Definitions - Data is defined consistently throughout the Trust, and the definitions are understandable and available to all users
- data Security - Data, whether stored, in transit or in use, is protected from unauthorised use and disclosure to ensure the required levels of confidentiality, integrity and accessibility
- interoperability - Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology

3.2 Data strategy

A vision statement and plan for data strategy shall be maintained. This sets priority and direction for data and data related activities. Such strategy will take into account the overall Trust approach for the deployment and development of its key resources: people, process, technology, data and space

3.3 Data access

Access to data will be limited to individuals that require the data to effectively complete their duties. This will mean that not all data is available to all individuals within the Trust at all times. Data access rights will be determined by the Executive Team and the Trust Board and reviewed on a regular basis.

3.4 Data usage

Data usage shall be limited to the individuals identified in the Data Access section and will only be used for the benefit of the Trust.

3.5 Data classification

The Data Governance Committee shall ensure that there is approved Data Classification, classifying each data element according to an agreed Trust definition; an example of this definition might be Highly Confidential (high risk), Confidential (high risk), Restricted (medium risk) and Public (low risk).

The Data Governance Committee shall oversee the Trust Data Model, including the definition of different types of Trust data, and defining the standard for documentation of data elements. This includes documenting data flows between systems and organisations so the origin of data elements can be traced through systems and processes.

3.6 Data collection and maintenance

The Data Governance Committee will assure the accuracy and quality of data (access control, backup, etc.) and implement programs for data quality improvement.

3.7 Data retention

The Data Governance Committee will ensure appropriate generation, use, retention, disposal, etc., of data and information consistent with Trust Policies, among them the Information Systems Security Manual and Guidelines and standards for disposal.

4.0 Relationship with existing policies

This policy forms part of the Trust's Data Policies. It should be read in conjunction with: the Information Systems Security Manual and Guidelines, Data Classification Policy and all supporting policies.

5.0 Roles and responsibilities

5.1 No one person, department, academy, or group "owns" Trust data, even though specific individuals bear some responsibility for certain data. The Trust owns the data (or in some cases, such as with bank accounts, is the custodian of data), but a specific person in the form of the Steward has ultimate responsibility to define management of the assigned data set within the scope of legal and regulatory obligations. The roles and responsibilities outlined below will govern management, access, and accountability for Trust data.

5.2 The Trust appoints senior level individuals as Data Stewards look after particular sets of data, such as "people data", "student data", and so on. For example the HR Lead is a suitable Steward for People Data.

5.3 Data Stewards shall appoint Data Custodians as required to assist in the execution of the data strategy, policy and procedures for their area of stewardship.

5.4 The Data Governance Committee will have oversight of data across the Trust. The committee will have responsibility for defining data policies, data standards and will respond to any issues relating to the data that the Trust holds. This committee will consist of:

- a member of the Executive who leads the design, implementation and continued maintenance of data control and governance across the Trust
- the Head of IT will ensure that the correct controls and systems are in place to support data governance across the Trust
- the Senior Data Managers who provide an oversight for solution designs and implementation
- the Data Protection Officer who will ensure adherence to required standards (legal, HR, GDPR)

5.5 The Data Governance Committee must be people that are able to make decisions and enforce these decisions throughout the Trust. Data Custodians can be appointed at academy level and will manage the gathering and storing of data (e.g. student records, admissions data, assessment data, employee records and so forth). The Data Governance Committee are ultimately accountable for the state of the data as an asset.

5.6 Data Stewards

Data Stewards will make sure that the data policies and data standards are adhered to on a daily basis at each academy or within each service area. These people will often be the subject matter experts for a data entity and / or a set of data attributes. Data stewards are either the ones responsible for taking care of the data as an asset or the ones consulted on how to do that. Further detail of this role can be found in Annex 1.

5.7 Data Custodians

Data Custodians are Trust employees and their staff who have operational level responsibility for the capture, maintenance, dissemination and storage of Trust Data. Further detail of this role can be found in Annex 1.

Everyone responsible for using data has to follow the six GDPR principles. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- maintained in an accurate state
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights whilst being kept safe and secure

All users of data have responsibility for preserving the security and integrity of Trust Data. Proper stewardship and custodianship of Trust Data will facilitate appropriate access to data. All data users must adhere to the following:

- **Confidentiality:** Respecting the confidentiality and privacy rights of individuals whose records they may access.
- **Ethics:** Observing the ethical restrictions that apply to data to which they have access.
- **Policy Adherence:** Abiding by applicable laws and Trust policies with respect to access, use, protection, proper disposal, and disclosure of data.
- **Quality Control:** Reviewing reports created from data to ensure that the analysis results are accurate and the data has been interpreted correctly.
- **Responsible Access:** Accessing and using data only as required in their conduct of Trust business. Reporting any breaches of Trust information in a timely manner according to procedures defined in the GDPR Policy.

Annex 1 - Definitions of roles

Title	Definition
Data Stewards	The Data Governance Committee shall appoint Data Stewards and ensure that all relevant Data Entities have a responsible Steward. Data Stewards look after particular sets of data, such as "people data", "student data", and so on. For example the HR Director is a suitable Steward for People Data. Data Stewards shall be responsible for the management of data under their oversight, under the direction of the Data Governance Committee. They shall appoint Data Custodians as required to assist in the execution of the data strategy, policy and procedures for their area of stewardship. Use of data from one domain by another (sometimes known as transformed data) shall comply with the direction of the steward for the data as per the source. For example, the rules, definitions and treatment of people data, wherever that data may be held shall comply with the rules, definitions and treatment established by the people data domain owner. Stewardship can be considered as: • taking responsibility for the survival and wellbeing of something that is valued • the responsibility for taking good care of resources entrusted to one Data Stewardship, is concerned with taking care of data assets that do not necessarily belong to the stewards themselves. Data Stewards represent the concerns of others. Some may represent the needs of the entire Trust. Others may be tasked with representing a smaller area: such as a faculty, academy or service. By virtue of their positions, Stewards of Trust Data have the primary administrative and management responsibilities for segments of Trust Data within their functional areas. Stewards of Trust Data implement policy, define procedures pertaining to the use and release of the data for which they are responsible, and ensure the feasibility of acting on those procedures. Stewards are responsible for defining procedures and making policy interpretations for their area. Any such specific items must, at minimum, meet Trust policy standards. They are responsible for coordinating their work with other Trust services and academies associated with the management and security of data, such as the Information Security Officer and IT staff. • Access: Approving requests for access to Trust Data within their functional area, specifying the appropriate access procedure, and ensuring appropriate access rights and permissions according to classification of data. • Communication: Ensuring that users of the data for which the Stewards are responsible are aware of information handling procedures. • Compliance and Data Security: The Steward is ultimately responsible for compliance with applicable legal and regulatory requirements, and with Trust policies and procedures, including specific policies or procedures established by The Data Governance Committee. Stewards must be knowledgeable about applicable laws and regulations to the extent necessary to carry out the stewardship role. Stewards must take appropriate action if incidents violating any of the above policies or requirements occur. • Data Classification: Classifying each data element according to the Trust definition – Highly Confidential (high risk), Confidential (high risk), Restricted (medium risk) and Public (low risk). • Data Lifecycle and Retention: Ensuring appropriate generation, use, retention, disposal, etc., of data and information consistent with Trust Policies, among them the Information Security Policy and standards for disposal. • Data Manipulation, Extracting and Reporting: Ensuring proper use of Trust Data and recommending appropriate policies regarding the manipulation or reporting of Trust Data elements and implementing procedures to carry out these policies. • Data Quality, Integrity and Correction: Ensuring the accuracy and quality of data (access control, backup, etc.) and implementing programs for data quality improvement. Consulting with data consumers / users to determine appropriate data sources. Determining update precedence when multiple sources for data exist. Determining the most reliable source for data.

Title	Definition
Data Stewards	• Data Storage: Documenting official storage locations and determining archiving and retention requirements for data elements. • Education (Training and Advice): Ensuring that education of employees responsible for managing the data is provided in reporting standards, data retention, data handling, and data security. • Policy Implementation: Establishing specific goals, objectives, and procedures to implement the policy and monitor progress toward implementation.
Data Custodians	Data Custodians are Trust officials and their staff who have operational level responsibility for the capture, maintenance, dissemination and storage of Trust Data. Stewards of Trust Data may appoint Custodians to assist with data administration activities. A Custodian of Trust Data is given specified responsibilities and receives guidance for appropriate and secure data handling from the Stewards. A Custodian has the responsibility for the day to day maintenance and protection of data. Specific responsibilities also include: • Access: With guidance from the respective Stewards and in collaboration with technical support staff; Custodians recommend appropriate procedures that satisfy specified information security requirements including legal and compliance obligations as well as applicable Trust policies. • Data Collection and Maintenance: Collecting and maintaining complete, accurate, valid, and timely data for which they are responsible • Data Security: Administering and monitoring access in collaboration with technical support staff, defining mitigation and recovery procedures. Reporting any breaches of Trust information in a timely manner in accordance with the GDPR Policy. • Documentation: Writing the documentation for each data element based upon stewardship requirements, policy, and best practices. This documentation will include, at a minimum, the data source, data provenance, data element business name, and data element definition. It should also include documentation of reporting processes, and the basis for data categorisations within these processes (for example, categorisation of student and staff activity, or of expenditure data). • Education (Training and Advice): At the direction of the Steward, providing education in data retention, data handling, and data security to employees responsible for managing the data.

Review

The Executive will monitor the application and outcomes of this policy on an annual basis to ensure it is working effectively and conforms to current legislation and advice. Any revisions will be presented to the Trust Board for approval.