Ascend Learning Trust

Records and Data Management Policy

Policy Owner:	Secondary Director of Education
Date of issue:	November 2024
Policy Level:	Tier 1
Approved by:	Full Trust Board
Next Review:	November 2025

Contents

Version Control

Version	Details	Author	Date
1.0	Template	DPE	19th May 2019
1.1		DPE	23rd May 2023
1.2		DPE	12th August 2024

Related Policies/Documents

- Ascend Data Protection Policy
- Ascend Acceptable Use Policy
- Retention Schedule

Policy Statement

Ascend Learning Trust (hereafter referred to as The Trust) will create, maintain and manage accurate, reliable and useable records in line to ensure the Trust has the information it needs to operate and to have information available when it is needed.

The Trust will formulate an information governance framework to ensure the information in the Trust's electronic and paper records:

- support the successful operations of the Organisation
- can be trusted
- contain only the minimum required information for the purpose of the information
- are properly maintained and organised
- are handled appropriately and in accordance with legal requirements and other guidance
- remain accessible, readable, authentic and up-to-date
- are kept securely, whatever the format
- can be easily found by those who need them
- only accessed by those permitted to view them
- support efficiency by avoiding duplication and only printing emails and electronic records when absolutely necessary
- are retained for a specified length of time and not indefinitely as retaining data can expose the Organisation to risk
- are disposed of securely as per the disposal schedule

1.1.

Failure to comply with this policy can expose the Trust to fines and penalties, failure of trust and adverse publicity, difficulties in providing evidence when we need it, responding to data subject access requests and in running our operations.

Complying with this policy helps the Trust comply with legislation and operate efficiently.

Policy Scope

This policy covers all data that we hold or have control over including where it is held by third-parties (e.g. cloud storage providers or offsite records storage).
This includes physical data such as:

- hard copy documents
- contracts and invoices
- notebooks
- letters
- invoices
- teacher, student and employee files
- hard copy media, including but not limited to photographs

It also includes electronic data such as:

- emails
- electronic documents
- electronic records held in databases
- audio and video recordings
- other electronic media, including but not limited to photographs
- CCTV recordings.

It applies to both personal data and non-personal data. In this policy, we refer to this information and these records collectively as "data".

This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

Who this policy applies to?

This policy is the responsibility of all staff including:

- Employees (permanent and temporary, agency and casual staff)
- Volunteers, students, interns and trainees doing placements within the Organisation
- Governors and Trustees
- Contractors conducting business with the Organisation
- Any other third-parties acting jointly or in partnership with the Organisation

Where it applies

Premises

- All premises operated by the Organisation
- Anywhere that any of those listed in "Who this policy applies to" conduct their work

Systems

- Any electronic system or database operated by, or on behalf of the Organisation

- Any computer system, peripheral equipment, software, memory devices, tablets and smartphones.

Roles and Responsibilities

We have a responsibility to ensure that our records are managed well.

Different staff have different roles in relation to records management and these responsibilities are detailed below:

CEO (at whole trust level) Headteacher (within an individual school context)	Overall accountability for records management and is responsible for ensuring compliance with legislation, regulation and guidance
COO (at whole trust level) School Business Manager or Office Manager (within an individual school context)	Provide support to the information process owners and act as a departmental point of contact for all records management matters. Overall responsibility for managing records management risks and for ensuring effective systems and processes are in place to deliver the information security agenda
Senior Leadership Team	Pro-actively promote records management awareness and mentor and train departmental staff in records management
Information Process Owners	Are responsible for ensuring that they comply with the records management policy and standards.
Board of Trustees	Responsible for agreeing on the records management policy and considering and approving changes to it, along with reviewing annual reports on records management matters.
All staff, contractors, consultants and third parties -	Everyone who receives, creates, maintains or has access to our documents and records is responsible for ensuring that they act in accordance with our records management policy, standards guidance and procedures.
Data Protection Officer	Responsible for assisting in monitoring compliance with this policy

	Responsible for advising staff on compliance with the procedures supporting this policy Responsible for assisting in the production of Privacy Impact Assessments

Information Classification

The Trust has established a framework for classifying, the appropriate handling and the use of data and information assets, based on its level of sensitivity, value and importance to the organisation.

Classification will aid in assigning security controls for the protection and use of data and information in order to ensure that data is created, stored, handled and destroyed appropriately to ensure controls can be put in place to make data available only to those authorised at any point during the data lifecycle.

More information regarding information classification is available in Appendix 1.

Retention Schedule

The Trust has established a retention schedule that outlines the processes around both retaining data and the length of time applicable to various types of data. After the specified period has ended, the data may be:

- Securely destroyed
- Anonymised
- Retained for historical or archival purposes
- Retained due to a valid business reason (e.g. for use in litigation, or in defence of a civil claim).

Documents may include personal and non-personal data. This policy applies to all data, not just personal data.

Data that is not held within a filing system (disposable data) should be securely destroyed once it no longer has a business use. This includes notebooks and diaries which should not be kept by individuals beyond their required business use.

If there is an omission in the Ascend Retention Schedule, or if you are unsure, please contact a senior member of staff or the Data Protection Officer.

Records (physical and electronic) that are relevant to current or potential legal proceedings, statutory investigation, audit, or any other relevant circumstances (including subject access requests), must not be deleted, disposed of, destroyed, or changed until determined those records are no longer needed.

Contact the Data Protection Officer if you are aware of contraventions of this policy or have any questions regarding retention schedules.

Data Storage, backup and destruction

All data must be stored in a manner that is safe, secure, accurate and accessible.

Records that are essential to business operations should have a backup and recovery strategy documented in the business continuity plan.

Information Process Owners are responsible for ensuring that data has met its required retention period and ensuring its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by a secure process such as shredding. Where shredding bags are used, they must be kept securely at all times until collected by authorised personnel and destroyed.

Non-confidential data may be destroyed by recycling.

The destruction of electronic data must be coordinated with the IT Department and where appropriate a certificate of destruction is obtained when the hardware is destroyed.

Data destruction must stop immediately where records (physical and electronic) are relevant to current or potential legal proceedings, statutory investigation, audit, or any other relevant circumstances. Data destruction should commence immediately when the embargo is no longer in place.

Information Process owners are responsible for ensuring that records under their control are kept up-to-date and accurate and should take measures to ensure record validity at regular intervals.

Appendix 1: Information Classification Guidance

The purpose of this guidance is to provide a framework for classifying, the appropriate handling and use of data and information assets, based on its sensitivity, value and importance to the Trust.

This guidance is applicable to all staff, stakeholders and authorized third parties who create, access, process or store information assets. This applies to personal data and non-personal data. Information assets are digital and non-digital data created, processed, stored, archived, deleted while executing business activities. Examples are database records, emails, source code, paper documents, designs, emails, databases, process data, images etc.

An Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organisation.

Data Classification

The classification of data helps determine what baseline security controls are appropriate for safeguarding that data.

The four levels are:

- Confidential
- Private
- Internal
- Public

Classification should be the responsibility of the document owner or other authorised individual.

	Confidentiality	**Integrity**	**Availability**
Definition	Confidentiality of information refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of	Integrity refers to the completeness and accuracy of information. Integrity is lost if changes are made to data or IT systems by either intentional or accidental acts, or if data is not up-to-date	Availability indicates how soon the information is required, in case it is lost or access disrupted. If critical information is unavailable to its end users, the organisation's

	confidential information can range from jeopardizing organisation security to the disclosure of private data of students or employees.	and accurate. If the integrity of data is not maintained, continued use of the contaminated data could result in inaccuracy, fraud, or erroneous decisions.	mission may be affected.
Public	Non-sensitive information is available for public disclosure. The impact of unauthorized disclosure **does not harm the organisation**. E.g. Newsletters or information published on the school website	There is **minimal impact** on the business if the accuracy and completeness of data is degraded.	There is **minimal impact** on the business if the asset/information is unavailable for up to 7 days
Internal	Information that can be shared internally with all staff, but is protected with limited control. The unauthorized disclosure of information here can cause **limited harm** to the organisation. e.g. Organisation charts, internal telephone directory.	There is a **moderate impact** on the business if the accuracy and completeness of data is degraded.	There is a **moderate impact** on the business if the asset/information is unavailable for up to 7 days
Private	Information belonging to the organisation and not for disclosure to the public and that has restricted	There is a **significant impact** on the business if the asset if the accuracy and	There is a **significant impact** on the business if the asset/information is

	access. The unauthorized disclosure of information here can cause **moderate harm** to the organisation. E.g planning documents, attendance records	completeness of data are degraded.	not available for up to 48 hours
Confidential	The information which is very sensitive or private, of highest value to the organisation and intended to use by named individuals only. **The unauthorized disclosure of such information can cause severe harm** (e.g. legal or financial liability, reputational damage). E.g. pupil safeguarding data, employee payroll data	The Integrity degradation is **unacceptable**.	The asset/information is **required on 24x7 basis**

Data Safeguards

The Trust and the owners of the information assets are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, labelling handling of, storage of, the transmission of, and disposal of print and electronic data.

Transmission

Transmission is the movement of data.

Confidential and Private data when transmitted externally should be sent via secure email or using encrypted and secure devices. Where possible, include data in a document and share this document using access control, rather than attaching as an email.

Internal data should be sent using authorised internal communication systems.

When sent physically, it should be sent via secure and recording postage or courier

Destruction

Data should be destroyed according to its importance:

Confidential, Private and Internal data:

Securely shred immediately, or place into locked secure containers until securely destroyed. Use of shredding bags without securing them (placing in locked cupboards) is considered insecure and breach of the confidentiality requirements of this document.

The organisation's IT Manager should implement procedures and technical measures for the secure destruction of electronic data and physical hardware.

Public data:

Can be placed in open recycling containers.