



Data Retention and Disposal Policy

Version Control						
Version	Author	Date	Changes	Approval	Approval Date	Review Date
1.1	L Storey-Aung	06/09/22	Policy creation	DW	07/09/22	06/09/2023
1.2	D Priestley	06/09/23	Policy review	DW	06/09/23	06/09/2024
1.3	D Priestley	06/09/24	Policy review	DW	06/09/24	06/09/2025
1.4	D Priestley	05/09/25	Policy review	DW	05/09/25	05/09/2026
1.4	D Priestley	29/09/26	Policy review	DW	01/10/26	01/10/27

DATA RETENTION AND DISPOSAL

POLICY STATEMENT

Aim2Learn Ltd (A2L) confirms that we are committed to the secure retention and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner.

We recognise and understand that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation.

We have specific measures for deleting and erasing personal information to ensure compliance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA18).

PURPOSE

The purpose of this document is to provide the Company's statement of intent on how we retain and dispose of secure information and confidential data in accordance with our legal, statutory and regulatory obligations. The Company ensures that we have: -

- A standardised approach to document retention
- a standardised and established approach to handling the disposal of confidential waste and information assets
- procedures in place for the disposal of secure waste; including hard copies, electronic formats and information assets
- a dedicated Retention & Erasure Policy within our GDPR/DPA18 program to comply with our data protection obligations
- guidance for staff on dealing with secure disposal and/or destruction
- controls and measures in place to comply with any regulatory or legal requirements as they relate to the disposal and destruction of confidential waste and hardware

SCOPE

This policy applies to all staff within A2L (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns

and agents engaged with A2L in the UK or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

OBJECTIVES

General Data Protection Regulation (GDPR)

A2L needs to collect personal information about the people we employ, work with, including learners and whom we have a business relationship with to effectively and compliantly carry out our everyday business functions and activities, and to provide the products and services defined by our business type. This information can include (but is not limited to), name, address, email address, data of birth, IP address, identification number, ULR Number, Telephone number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation, UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle:

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

A2L have put into place numerous principles and processes for handling the disposal of confidential waste materials and information assets (information and physical), as detailed below. A2L ensures that: -

- We have a standardised and established approach to retention of documents and handling the disposal of confidential waste and information assets
- We have procedures in place for the disposal of secure waste, both hard copies and electronic formats and information assets
- We provide guidance for staff on dealing with disposal and/or destruction
- We have robust controls and measures in place to comply with any regulatory or legal requirements as they relate to disposal and destruction
- Secure waste bins are used for sensitive and/or confidential wastepaper
- Confidential paper is never used a scrap or re-printed onto
- Confidential wastepaper is never placed into the general waste bin or outside disposal receptacle unless it has been securely shredded

- Waste will be stored in accordance with the waste disposal procedures if not collected immediately, that includes being locked away securely if left overnight, or in an unoccupied building
- Physical and IT assets are encrypted and/or reformatted prior to disposal
- The IT Manager must provide authorisation for assets removal and disposal
- Assets are disposed of in accordance with the manufacturer's guidelines
- Assets, equipment and information are disposed of in an authorised, appropriate, legal and environmentally sound manner adhering to appropriate standards or codes of conduct for Cyber Essentials.

GUIDELINES & PROCEDURES

Records management training is mandatory for all staff as part of A2L's statutory and compliance training programme and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be created, maintained and retained in order to provide information about, and evidence of transactions, customers, employment and activities.

It is our intention to ensure that all records and the information contained therein is: -

- Accurate - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- Accessible - records are always made available and accessible when required (with additional security permissions for select staff where applicable to the document content)
- Complete - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- Compliant - records always comply with any record keeping legal and regulatory requirements
- Monitored – staff, company and system compliance with this Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All A2L employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within A2L, we: -

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained

- Establish and verify retention periods for the data, with special consideration given in the below areas: -

- the requirements of A2L
- the type of personal data
- the purpose of processing
- lawful basis for processing
- the categories of data subjects

- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, A2L will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices

- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered

- Transfer paper-based records and data to an alternative media format in instances of long retention periods (with the lifespan of the media and the ability to migrate data where necessary always being considered)

Once a record, document or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR/DPA18 requirements or to archive records for a further period.

DESTRUCTION AND DISPOSAL OF RECORDS & DATA

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

PAPER RECORDS

Due to the nature of our business, A2L retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. A2L utilise Onsite-Shredding to dispose of all paper materials.

Shredding machines and confidential waste sacks are made available throughout the building and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

ELECTRONIC & IT RECORDS AND SYSTEMS

A2L uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

Only the IT Manager can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, the IT Manager must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Manager is responsible for updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and the IT Manager to ensure that all relevant data has been sufficiently removed from the IT device and where applicable, backed up, before requesting disposal and/or prior to the scheduled pickup.

DISPOSING OF REMOVABLE MEDIA DEVICES

When A2L no longer has use for any removable media devices or where they are no longer functioning due to damage or corruption, they are securely disposed of to protect any remaining information and prevent data leakage or unauthorised access. All types of removable media are given to the IT Manager for disposal and no employee is permitted to carry out this process themselves.

The IT Manager formats all media types and ensures that information and materials have been fully removed from the device prior to disposal. However, as technology advances, A2L are aware that methods can exist to retrieve partial data or imprints from removable media and as such, secure disposal methods are still used as well as encryption techniques. The IT Manager has access to specialist software and tools for the erasure, formatting and

disposal of removable media types or where this is not possible, A2L employs a professional service provider to carry out this task.

RESPONSIBILITIES

A2L will ensure that all staff are provided with the time, training and support to learn, understand and implement this Secure Disposal Policy and subsequent procedures. Management are responsible for a top down approach and in ensuring that all staff are included and have the support needed to meet the regulatory requirements in this area.

