



Document Storage and Retention Policy

Atlas Star IT Centre

Purpose

This policy outlines the principles and guidelines for the secure storage, retention, and disposal of documents containing personal data and academic qualifications at Atlas Star IT Centre. The policy ensures compliance with legal, ethical, and institutional requirements for data protection and document management.

Scope

This policy applies to all employees, staff, and learners of Atlas Star IT Centre and covers all documents, whether in physical or electronic format, that contain personal data or information about academic qualifications.

1. Types of Documents Stored

The following categories of documents are stored by Atlas Star IT Centre:

1. Staff Records:

- Personal identification (e.g., passports, IDs, visas)
- Employment contracts and related documents
- Payroll records
- Performance reviews and disciplinary records

2. Learner Records:

- Personal identification (e.g., IDs, birth certificates)
- Academic qualifications (certificates, transcripts)
- Enrolment forms and contracts
- Attendance and progress records

3. General Administrative Records:

- Financial documents (invoices, receipts)
- Internal policies and procedures
- Health and safety compliance documentation



2. Retention Periods

The retention periods for different types of documents are defined below:

| Document Type | Retention Period | Rationale |
|----------------------------------|----------------------------------|-------------------------------|
| Staff personal identification | 7 years after employment ends | Legal and audit requirements |
| Staff employment contracts | 7 years after employment ends | Legal compliance |
| Learner personal identification | 5 years after program completion | Data protection requirements |
| Learner academic qualifications | Permanent | Future verification needs |
| Attendance and progress records | 5 years after program completion | Academic and legal compliance |
| Financial documents | 7 years | Tax and audit requirements |
| Internal policies and procedures | Until superseded | Operational efficiency |
| Health and safety documents | 7 years | Legal compliance |

3. Document Storage

3.1 Physical Documents

- **Storage Location:** Secure cabinets within access-controlled areas.
- **Security Measures:**
 - Locked filing cabinets accessible only to authorized personnel.
 - Secure disposal through shredding or incineration when documents reach the end of their retention period.

3.2 Electronic Documents

- **Storage Location:** Secure, encrypted servers managed by Atlas Star IT Centre.
- **Security Measures:**
 - Role-based access control (RBAC).
 - Regular backups stored offsite with encryption.
 - Use of multi-factor authentication (MFA) for access.
 - Periodic security audits and vulnerability assessments.



4. Security and Confidentiality

Atlas Star IT Centre prioritizes the confidentiality, integrity, and availability of all stored documents. Measures include:

- Compliance with data protection laws (e.g., GDPR, Data Privacy Act).
- Staff training on secure document handling practices.
- Immediate reporting and mitigation of any data breaches.

5. Disposal of Documents

At the end of the retention period, documents will be disposed of securely:

- **Physical Documents:** Shredding or incineration.
- **Electronic Documents:** Permanent deletion using secure erasure tools.

6. Responsibilities

- **Administration Team:** Responsible for maintaining, reviewing, and securely storing records.
- **IT Team:** Ensures electronic document security, backup, and secure disposal.
- **Staff and Learners:** Responsible for providing accurate information and adhering to institutional policies.

7. Policy Review

This policy will be reviewed annually or as required to ensure compliance with applicable laws and best practices.