



Holden Knight Recruitment Ltd

Secure Document Storage & Management Policy

Human Resources v1.2

Review Date: November 2027



SECURE DOCUMENT STORAGE & MANAGEMENT POLICY

1. Purpose

- 1.1 This policy outlines Holden Knight Group's approach to the secure storage, handling, and retention of both electronic and physical documents. It complements the Information Security Policy and ensures all documentation is managed in a manner that protects confidentiality, maintains integrity, ensures availability, and meets legal, contractual, and regulatory obligations, including compliance with UK data protection laws.

2. Scope

- 2.1 This policy applies to all staff and contractors employed by Holden Knight Recruitment. It includes:
- Electronic documents stored on company systems
 - Hard copy (physical) documents
 - Documents containing personal, client, financial, or proprietary information
- 2.2 This policy also extends to any documentation related to safeguarding, health, education or support services for children and vulnerable adults, ensuring full compliance with relevant statutory responsibilities.

3. Storage of Electronic Documents

3.1 Approved Platforms

All electronic documents must be stored using approved systems:

- Microsoft 365 (OneDrive, SharePoint)
- Microsoft Azure-hosted storage

- 3.2 These platforms are protected using encryption, access control, and backup protocols in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

3.3 Security Measures

- Data at rest is encrypted using Azure Storage Service Encryption (SSE)
- Data in transit is encrypted using TLS 1.2 or higher
- Access to documents is based on the principle of least privilege
- MFA is required for access to all cloud systems
- Version history is enabled to track document changes
- Regular backups ensure recovery in case of data loss

3.4 Access Control

- Role-based permissions ensure users only access relevant documents
- Document access is reviewed regularly by the Chief Technology Officer (acting as interim Data Protection Officer)

- Access is revoked promptly upon role changes or offboarding

3.5 **Document Sharing**

- Documents may only be shared externally using secure Microsoft 365 features
- Links with time-bound access and view/edit restrictions are required
- Sharing of personal data must comply with data minimisation principles under UK GDPR

3.6 **Special Category Data**

- Special category data, including safeguarding records or health-related documentation, is handled in accordance with Article 9 of UK GDPR
- This data is stored and accessed with the highest level of security controls and oversight

4. **Storage of Hard Copy Documents**

4.1 **Physical Security**

- Sensitive documents are stored in locked cabinets within secure office areas
- Access to physical records is restricted to authorised personnel only
- Offices are protected by access control systems during and after working hours

4.2 **Handling Procedures**

- Documents must not be left unattended in public or unsecured areas
- Printing of sensitive documents is discouraged unless necessary
- Printed documents must be collected immediately from printers

4.3 **Disposal**

- Hard copies must be disposed of via cross-cut shredders or secure document disposal services
- Disposal logs are maintained for high-sensitivity records
- Disposal practices comply with the data erasure principles of UK GDPR

5. **Document Retention**

5.1 **Retention Periods**

Retention schedules are based on regulatory, legal, and business requirements:

- HR records: 7 years
- Client contracts: Minimum of 6 years after contract end
- Safeguarding and compliance records: As specified by regulators or commissioning bodies

- Financial documents: 6 years (as per HMRC requirements)

5.2 Archiving

- Archived documents are labelled, dated, and stored in secure digital or physical formats
- Archived electronic files must remain accessible but segregated from active files

5.3 Review and Disposal

- Retained documents are reviewed annually
- Records past retention limits are securely deleted or destroyed
- Disposal is documented and complies with the right to erasure under UK GDPR where applicable

6. Responsibilities

6.1 Chief Technology Officer (acting as interim Data Protection Officer):

Oversees implementation and review of document storage and data protection policies

6.2 Operations Team:

Acts as the first point of contact for any suspected breaches or document security concerns

6.3 Department Heads:

Ensure staff follow approved storage practices

6.4 All Staff:

Responsible for handling documents securely and reporting incidents

6.5 Data Protection Officer (DPO)

The Data Protection Officer (DPO) has formal responsibility for data governance and secure document management.

7. Monitoring and Compliance

- Random audits may be conducted to verify compliance
- Non-compliance may result in disciplinary action
- Document storage practices will be reviewed alongside the Information Security Policy annually
- All procedures within this policy align with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant ICO guidance
- Holden Knight Group maintains procedures for responding to Subject Access Requests (SARs) and Freedom of Information Requests (FOIs) where applicable, ensuring timely and lawful responses

- Any data shared with or processed on behalf of third parties, including local authorities and educational institutions, will be governed by a formal Data Processing Agreement in compliance with Article 28 of UK GDPR
- Holden Knight Group follows recognised Information Sharing Protocols (ISPs) when working with local authorities or partner agencies, ensuring that all data sharing is lawful, necessary, proportionate, and documented