BuildASkill Ltd
Building for the Future

Document Retention and Secure Storage Policy

Date 09/08/21
Reviewed 21/10/25
Date of next review 20/10/26

Contents

Summary 2

Scope 2

Introduction 2

Scope 2

Legislation and compliance framework 3

Responsibilities 3

Related policies 4

Standards 4

Management of records 5

Creating records 5

Organising records 5

Security and access 6

Retention 6

Disposal 7

Reappraisal 7

Permanent Preservation 7

Destruction 7

Records of disposal 8

Disposal of IT equipment 8

Summary

This Policy establishes principles for ensuring that BuildASkill Ltd implements effective records management, accounting for legislative, regulatory and best-practice requirements. It provides guidance on the retention and disposal of records held by BuildASKill Ltd.

Scope

The policy applies to all employees of BuildASKill Ltd, including contractors, temporary staff and volunteers.

Introduction

Records Management is the process of managing records, in any format or media type, from creation through to disposal in line with legal and business requirements. Effective Records Management allows for fast, reliable and secure access to records ensuring the timely destruction of redundant records as well as the secure identification and archiving of records considered worthy of permanent preservation.

BuildASKill Ltd recognises that the efficient management of records throughout their lifecycle is necessary to support its core functions, to comply with its legal and regulatory obligations.

This policy sets out principles for ensuring that BuildASKill Ltd implements effective records management, and provides guidance on the retention and disposal of records. It covers all types of records created or used by staff, whatever format they are held in, and addresses the requirements of the Lord Chancellor's Code of Practice on the Management of Records (issued under Section 46 of the Freedom of Information Act 2000).

Scope

This policy applies to all records created, received, maintained and held, in all formats, by staff of BuildASKill Ltd in the course of carrying out their corporate functions. Records are defined as documents, regardless of format, which facilitate the operations and business of BuildASKill Ltd and which are thereafter retained for a set period to provide evidence of its activities and transactions.

This policy applies to all employees of BuildASKill Ltd, including contractors, temporary staff and volunteers. It is a contractual obligation to adhere to the requirements of the policy.

Legislation and compliance framework

The management of records held by BuildASKill Ltd is regulated by the following legislation:

- Data Protection Act 2018 & General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Limitation Act 1980

The Data Protection and Freedom of Information Acts contain provisions relating to the destruction or alteration of information or records after a legal access request has been received. Such destruction or alteration will be considered a disciplinary offence. The Freedom of Information Act 2000 also creates a criminal offence in relation to these actions. The Section 46 Code of Practice on the Management of Records sets out measures and good practice that should be in place in relation to information management to ensure that requests made under the Freedom of Information Act can be answered in a timely manner, and also that information is not disposed of when it may still be required.

The ISO 15489 series of international standards on information, documentation and records management establishes standards for the management of business records.

Other areas of the company's operations have specific retention requirements set out in separate legislation such as those relating to employment, health and safety, finance and pensions, and environmental information. BuildASKill Ltd also requires high quality records to be maintained for the purposes of audits and reviews by regulatory bodies.

Responsibilities

BuildASKill Ltd has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment.

Line managers are responsible for ensuring that their staff are aware of this Policy and comply with its requirements. All members of staff are responsible for ensuring that their work is documented appropriately, that the records which they create or receive are accurate and managed correctly, and are maintained and disposed of in accordance with the companies guidelines and any legislative, statutory and contractual requirements. Line managers should ensure that when a member of staff leaves, responsibility for their records is transferred to another person; if any of the information is redundant, it should be deleted by either the departing member of staff or their line manager.

It is vital that records management considerations are appropriately incorporated into project and planning processes and system design at the earliest possible stage of development. Where records contain personal data there is a legislative requirement to do this in order to ensure that a data protection by design and default approach is followed.

Related policies

The Policy should be considered in conjunction with the following policies and procedures:

- Data Protection Policy
- Privacy Policy

Standards

The following standards need to be maintained at all times:

• Records must be managed in a manner complying fully with legislative and regulatory requirements affecting their use and retention.

• Records must have relevant content, context and format, and must be accurate, authentic, useable, reliable, timely and well managed.

• Records must directly relate to and support a service, function or activity delivered by BuildASKill Ltd, and be able to support decision-making.

• Records must serve the interests of the company, its staff, learners and other stakeholders by maintaining high quality documentation for appropriate lengths of time.

• Records must be managed via systems and processes ensuring efficiency and consistency throughout their lifecycle of creation, distribution, use, maintenance and disposition.

• Records must be managed and stored in a suitable format to retain quality, relevance, accessibility, durability and reliability. Any transfer to another format must have due regard to retaining these qualities.

• Records must be kept securely as befits the confidentiality and importance of the content, being protected from unauthorised or unlawful disclosure.

• Records must be accessible and retrievable as required to support business efficiency and continuity.

• Records must be retained or disposed of in compliance with the Records Retention Schedule.

• Records must be subject to clearly defined arrangements for appraisal to select those worthy of permanent preservation. Those of historical significance to the corporate memory of the organisation should be preserved.

• Records must undergo appropriate destruction when no longer required, in an organised, efficient, timely and (where necessary) confidential manner.

Management of records

Creating records

Each department of BuildASKill Ltd must have in place adequate systems for documenting its principal activities and ensuring that it creates and maintains records that serve its functions and the standards detailed above.

The records must be accurate and complete, so that it is possible to establish what has been done and why. The quality of the records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met. The integrity of the information contained in records must be beyond doubt; it should be compiled at the time of the activities to which it relates, or as soon as possible afterwards, and be protected from unauthorised alteration or deletion.

Where appropriate, templates should be used, so that documents are produced consistently and quickly. In addition, version control procedures are required for the drafting and revision of documents, so that staff can easily distinguish between different versions and readily identify the latest copy.

The retention of duplicate records presents enhanced risks regarding their management, use and alteration. Whereas there may be a need to keep local versions of records held centrally, it should be avoided where possible and a system enabling use of a single central version implemented. Where practical, to reduce the need for duplication documents should be stored in central folders that are accessible by relevant staff. Digital information should be filed in shared workspaces wherever possible. File titles should be brief but comprehensible with a consistent format used.

Where possible, both paper and electronic records systems should contain metadata (information about the structure of the records system or series) to enable the system and the records to be understood and operated efficiently, providing an administrative context for effective management of the records, and to enable individual records to be identified and accessed efficiently. The metadata could include details of the structure of the records, dates of access, use, alterations, disposal etc.

Organising records

Records should be organised and described in a uniform, logical manner that facilitates fast, accurate and comprehensive retrieval so that they are easily accessible when required. A filing structure or records series should be used, i.e. a group or unit of related records, documents or information that is normally filed or kept together because they relate to a particular subject or function, or result from or document a particular activity.

Classifying records and holding them in an appropriate structure or scheme will enable suitable retention periods to be assigned. Keeping diverse records together in a less structured manner makes it more difficult to identify and retrieve them when required, and to apply responsible retention policies.

Standardised referencing and titling must be employed, so that information can be readily

identified and retrieved. Naming conventions will assist with using consistent terminology to improve efficiency. Titles given to digital and hard copy records and files should describe the content or subject matter accurately and helpfully.
Digital storage solutions enabling more sophisticated tagging and searching functionality will become more widely available for BuildASKill Ltd staff to use. These developments will assist with the correct storage, classification and retrieval of records.

Security and access

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. All records in any format must be held in accordance with the BuildASKill Ltd 's Data Protection Policy. Records must be stored in a safe and secure physical and digital environment taking account of the need to preserve important information in a useable format enabling access commensurate with frequency of use.

Records should not be only accessible by a single person but should be stored in centralised storage or filing systems or on a shared drive, so that departments can operate efficiently when individual members of staff are absent. Where appropriate, access to central records should be appropriately available across the company in order to avoid recreating information that already exists and storing duplicate data unnecessarily.

Records that would be vital to the continued functioning of BuildASKill Ltd in the event of a disaster must be identified and protected. These include records that would recreate the companies legal and financial status, preserve its rights, and ensure that it continues to fulfil its obligations to its stakeholders. All critical business data must be protected by appropriate preservation and backup. Where vital records are only available in paper format it is best practice that they are duplicated, and the originals and copies stored in separate locations. If, however, duplication is either impracticable or legally unacceptable, fireproof safes should be used to protect vital documents.

Retention

The Freedom of Information Act Section 46 Code of Practice on the Management of Records states:

"As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used and costs are not incurred in maintaining records that are no longer required."

Records must only be kept for as long as is required to meet operational, business and legal needs. It is a legal requirement established by the Data Protection Act to only retain records containing personal data for as long as is strictly necessary, and organisations can be subject to enforcement action for failing to comply. By having clearly defined procedures for the retention and disposal of records, BuildASKill Ltd can demonstrate corporate responsibility in the management of its information and records.

Record owners are responsible for ensuring that the retention periods are regularly reviewed (at least annually) to determine whether any retention periods applying to information within their department have expired. Once the retention period has expired, relevant action must be taken. Retention can be complicated if records of a dissimilar nature, with different retention requirements, are filed together. Departments should consider retention periods when designing their records storage systems and practices to avoid this issue. Files should be weeded regularly to ensure records are not kept for too long. If there is no alternative, the entire file should be retained for the longest relevant retention period.

Disposal

When a record reaches the end of its retention period a decision must be taken on its disposal, with the three possible outcomes:
a) Reappraisal
b) Permanent preservation / archival
c) Destruction

Reappraisal

Before action is taken to permanently preserve or destroy a record at the end of its retention period, a reappraisal of any need to retain it for present functions should be undertaken, but it should only be necessary to attribute a revised retention period on rare occasions.

In some circumstances it may be necessary to retain a record for longer than its defined retention period. A new operational function requiring its retention may have arisen, or it may be required for investigation or litigation purposes, or because it is needed in order to respond to an access request received under data protection or freedom of information legislation. If a record needs to be retained for longer, then a new retention timescale should be assigned to it. It is recommended that this date should not be too far in the future, enabling regular review of the decision while taking circumstances into account. A period of one year is recommended.

Permanent Preservation

If electronic records have been identified as having archival value then consideration should be given to whether they are retained in a format deemed to be future proofed, and how they can be transferred and stored for permanent preservation.

Destruction

Records must be destroyed in a timely and secure manner, and that senior staff within the relevant department are aware that the destruction is taking place. All copies, including security copies, preservation copies and where possible backup copies, held in any format must be destroyed at the same time.

Staff with access to digital records that are being deleted should ensure that any copies held anywhere in their email folders, files stores and recycle bin are also deleted to ensure completion. Items held in these locations are still held for the purposes of the Data Protection and Freedom of Information Acts. Deletion of an electronic file removes the link to

the file but it is possible that the file contents could still be retrieved using technical measures. Consequently, adequate security must continue to be applied to file locations and devices used to hold them until they have been fully expunged or wiped.

System backups will continue to hold copies of deleted digital records until such time that the backup is deleted. Whereas the requirements of the Data Protection and Freedom of Information Acts technically still apply to such records, the Information Commissioner's Office have taken a pragmatic approach to this type of content, recognising that it is possible to put it 'beyond use' while still held so rendering it out of scope. This will only apply if there is no intention to access or use it again, and it would require disproportionate effort to retrieve. However, such records could still need to be retrieved if subject to a court order.

Records of disposal

For potentially significant information a record should be kept of what has been disposed of, why it was disposed of and who authorised it, covering both destruction and transfer to archive. This will ensure there is a transparent audit trail detailing evidence of records that have been destroyed in line with BuildASkill Ltd.'s stated procedures.

Disposal of IT equipment

All disposal of IT equipment must be done securely and any information remaining on any storage device must be securely wiped.