**Records Management Policy**

*IMPORTANT NOTICE*

*This policy does not constitute legal advice. The policy should be tailored to reflect the Employer’s specific requirements following a data audit in accordance with the legislation, guidance and Codes of Practice issued by the Information Commissioner. This policy is designed to be used in conjunction with a Data Retention Policy and a Data Security Policy, which will be standard across your organisation and not specific to HR.*

**Records Management Policy**

1. **Introduction**

Maintaining business records in a systematic and reliable manner is essential to comply with our legal and regulatory requirements, e.g. relating to data protection, tax and employment. It also reduces the costs and risks associated with retaining unnecessary information.

This record management policy has been developed to help staff properly manage the records of [*insert organisation name*]. It sets outs:

what records are

how records should be classified and stored

how long different classes of record should be retained

how records should be disposed of

1. **Responsibility and application**

[*Insert name, department or role holder*] is responsible for this policy.

This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers. All staff must be familiar with this policy and comply with its terms.

This policy does not form part of any employee’s contract of employment and [*insert organisation name*] may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

1. **What are records?**

For the purposes of this policy, records are documents, communications and other materials that are written, recorded or otherwise machine readable. Records can exist in different formats including electronic, paper, book, facsimile, film, videotape, audiotape, and other formats available through existing and emerging technologies.

Voicemail, text or instant messages do not constitute records, except those that have been recorded and retained for business or regulatory purposes [e.g. texts relating to HR issues].

There are two types of records: business records and short-term records.

**Business records**

Business records are records created or received in the course of [*insert organisation name*]’s business that:

document a business-related event or activity

demonstrate a business transaction

identify individuals who participated in a business activity

support a business-related event, activity, or transaction, or

are needed for other legal, business, or compliance reasons

Business records must be properly classified, stored, retained and disposed of in accordance with this policy.

**Short-term records**

Short-term records are those with no enduring business or operational value, and which are not considered to be business records. These include:

general company-wide, division-wide or departmental announcements, notices or updates

unsolicited vendor bids and/or offers

unsolicited **[**CVs OR resumes**][** sent to non-HR personnel**]**

routine and general correspondence having only an immediate or short-term value, and

personal files, emails or other documents.

As a general rule, short-term records should be retained for no longer than [*insert number, eg 30*] days. While they may be captured by routine backup processes, they should not be specifically stored at an off-site storage facility. On occasion, it may be necessary to retain short-term records for longer than 30 days, eg [*insert example, eg confirmation of a team Christmas lunch booked several months in advance*]. However, once the record is no longer needed, it should be destroyed promptly.

Short-term records, including any personal files, emails or other documents on company premises or systems, may become business records if they are relevant to a legal or business matter of [*insert organisation name*].

1. **Creation of records**

The individual or department that authored, created or is the primary custodian of a record is responsible for ensuring it is retained and destroyed in accordance with this policy.

All records and other communications pertaining to [*insert organisation name*]’s business are to be appropriately and accurately worded. You must act responsibly, lawfully and professionally when creating records regarding our business activities and/or on our systems.

[*Insert organisation name*] prohibits staff from creating records that are misleading, intentionally false, fraudulent, sexually explicit, abusive, offensive, harassing, discriminatory, profane, libellous, defamatory, unethical, or that violate any laws, regulations or internal policies.

1. **Classification and mark-up of business records**

Some business records require greater levels of protection than others. Business records must be appropriately classified and marked to ensure a level of protection commensurate with their confidentiality, sensitivity or importance to the company.

**Classification of business records**

Business records are classified as:

restricted, and/or

confidential, or

general, or

public

It is not possible to list every possible type of record and say how it should be classified. Instead, you should consider the following questions and exercise your judgement.

|  |  |
| --- | --- |
| Does the record include personal data? | See our Data protection policy for a definition, but as a general guide this is data which identifies or can be used to identify an individual (the ‘data subject’).Records that contain personal data must be classified as restricted and confidential.  |
| Are we under an obligation to store, transmit, or delete the information in the record in a certain manner?  | This obligation could be imposed by a regulator or a contractual agreement with a supplier or customer, eg [*insert an example relevant to your business*]. |
| What is the commercial or competitive value of this information? | Information that would be valuable to our competitors such as trade secrets, strategic plans, pricing information, or merger and acquisition activity must be classified as confidential. |
| What is the potential impact if the record is inadvertently disclosed, corrupted, lost or destroyed? | Classify records as either restricted or confidential if inadvertent disclosure or loss etc would have an adverse impact on: —an individual—our reputation, competitive position, revenue**[** or share value**]** or—any of our customers, agents, suppliers or other partners |
| Is the record in the public domain? | Provided the record is in the public domain for legitimate reasons, eg not as a result of breach of confidence, the record should be classified as public. |
| [*Insert other factor*] | *[Insert outcome]*. |

See Appendix 1 for examples of how different records may be classified. If in doubt, consult [*insert eg your manager or a member of the legal team.*]

**Mark-up of business records**

Records classified as restricted or confidential must be marked as ‘Restricted’ and/or ‘Confidential’ in one or more of the following ways:

in the document header or footer

in the subject line of an email and/or the top or bottom of the body of the message

by way of a watermark in the Word, Adobe, PDF etc version of the document

by way of a stamp on the hard copy

[*insert other*]

In certain circumstances it may be necessary to expand on the mark-up, eg:

‘Restricted: do not forward, print or copy’

‘Restricted: encryption required’

‘Restricted: legal professional privilege’

The mark-up should be displayed on the front page and each subsequent page of the record.

1. **Retention of business records**

Business records must be retained as long as required by relevant laws and regulations and in accordance with [*Insert organisation name*]’s business needs.

**Retention periods**

Our record retention schedule at **[**[*insert where this can be found*] OR Appendix 2**]** sets out how long records will normally be held and when the record will be destroyed. We periodically review and update the schedule with additional record types.

Business records should not be disposed of or destroyed before the relevant retention period expires.

Business records should not, however, be kept longer than the relevant retention period unless the retention period for that particular record has been suspended, as described at section 10 below.

Where more than one retention period applies to a record, it should be retained in accordance with the longest retention period, unless otherwise directed by [*insert who, the Data Protection Officer*].

If a record type is not listed in the record retention schedule and is not a short-term record (see 3.5 above), contact [*insert who, eg the Data Protection Officer*] for guidance.

The following are not subject to the record retention schedule:

IT system backups—these are designed for operational restoration purposes and are not to be used for the retention of business records

emails of former employees that do not constitute business records—these may be retained for transitional or other business purposes, but are to be disposed of within 1 year of the date of employee’s termination, except as may be required under a litigation hold (see section 10.2).

**Retention: drafts and duplicates**

Draft or duplicate copies of business records should be retained only while they are needed for valid business reasons and never longer than the applicable retention period in the record retention schedule. For more guidance, see our Version control and document management policy.

You should not send draft or duplicate records to an off-site storage facility without the approval of [*insert who, eg a member of the in-house legal team*].

**Retention: format**

Most business records can be retained exclusively in electronic form and hard copies do not usually need to be retained.**[** The exceptions to this are:**]**

|  |  |
| --- | --- |
| [*insert document description, eg share certificate*] | [*eg A share certificate is prima facie evidence of ownership*] |
| [*insert document description, eg any registrable document, such as a document to be registered with HM Land Registry*] | [*explain why the hard copy cannot be deleted, eg The original should not be destroyed until the registration is complete and confirmed*] |
| [*insert document description*] | [*explain why the hard copy cannot be deleted*] |

For these types of record we must retain the hard copy **[**and the electronic version**]**.

Contracts and other legally binding records can be retained exclusively in electronic form, so long as the electronic record:

accurately reflects the original, and

is in a form that is capable of being retained and accurately reproduced for later reference throughout the required retention period

You should check with [*insert who, eg DPO*] before retaining contracts or other binding records solely in electronic form.

1. **Storage of records**

All records covered by the Version control and document management policy must be managed and stored in accordance with its terms.

Business records must be stored on [*insert organisation name*]’s premises or at a secure location or website approved by [*insert organisation name*] to provide physical or electronic storage facilities. See Appendix 1 for guidance on the level of security required for different classes of records.

The following records should not be retained at an off-site storage facility:

short-term or other non-business records

paper duplicates or convenience copies, or

authoritative **[**electronic**]** records where no duplicates exist—these should be stored [*state where or how*]

When archiving paper records at an approved storage facility, you must clearly label storage boxes as follows:

[*insert first part of your storage labelling protocol, eg record type*]

[*insert next part of your storage labelling protocol, eg matter type*]

[*insert next part of your storage labelling protocol, eg dept*]

designated destruction date consistent with the Schedule

1. **Removal of business records**

You may remove business records from [insert organisation name]’s premises only for legitimate business purposes; you must return those records when no longer needed off-site for business purposes.

1. **Destruction of business records**

Business records must be destroyed at the end of the relevant retention period, unless the retention period has been suspended under section 10.

See Appendix 1 for guidance on the method of destruction required for different classes of business record.

As a general rule, short-term records should be retained for no longer than [*insert number, eg 30*] days. While they may be captured by routine backup processes, they should not be specifically stored at an off-site storage facility. On occasion, it may be necessary to retain short-term records for longer than 30 days, eg [*insert example, eg confirmation of a team Christmas lunch booked several months in advance*]. However, once the record is no longer needed, it should be destroyed promptly.

Periodically, you should determine whether you have records in your control that should be discarded or destroyed pursuant to this policy.

If you have questions or concerns about retaining any records beyond the scheduled retention periods, you should contact [*a member of the in-house legal team*] before disposing of the records in question.

1. **Suspending the destruction date**

If a claim, audit, investigation, subpoena or litigation has been asserted or filed by or against [*insert organisation name*], or is reasonably foreseeable, we have an obligation to retain:

all relevant records, including those that otherwise would be scheduled for destruction under the records retention schedule, and

records that otherwise could have been disposed of as short-term records

On learning of an actual or reasonably anticipated legal action, the [*insert who, eg in-house legal team or Risk Partner*] will notify relevant staff to suspend disposal and destruction of applicable records. This is known as ‘litigation hold’.

If you become aware of an actual or anticipated claim, audit, investigation, subpoena or litigation, you must immediately report the matter to [*insert who, eg in-house legal team or Risk Partner*] and discontinue any scheduled disposal pending confirmation of whether litigation hold is required.

You must carefully and diligently comply with any litigation hold notices. In particular, you must not alter, dispose of, discard or destroy any records that are subject to litigation hold. You must also continue to retain any and all such records until the [*insert who, eg in-house legal team or Risk Partner*] issues a notice indicating that the litigation hold has been lifted and that the retention and disposal of such records should resume in accordance with [*insert organisation name*]’s retention schedule.

1. **Failure to comply**

[*Insert organisation name*] takes compliance with this policy very seriously. Failure to comply puts both staff and [*insert organisation name*] at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

Staff with any questions or concerns about anything in this policy should not hesitate to contact the [*insert relevant department or role holder*].

1. **Monitoring and review**

[Insert name, department or role holder] has overall responsibility for this policy. They will monitor compliance with this policy regularly to make sure it is being adhered to.

**Appendix 1**

**Classification mark-up and storage examples**

| Record classification | Examples | How should the record be marked-up? | Security and destruction |
| --- | --- | --- | --- |
| Restricted | Personal and sensitive personal data, eg HR records.Records containing **[**consumer OR **[**client**]]** information that is regulated by law, eg [*credit card details*].Records where disclosure will be high impact for the business of the data subject if disclosed.—[*insert example*]—[*—insert example*] | ‘Restricted’ or, as required:‘Restricted: do not forward, print or copy’‘Restricted: encryption required’‘Restricted: legal professional privilege’‘Restricted: without prejudice’‘Restricted: do not forward, print, or copy’‘Restricted: named recipients only’NB: Records that contain personal data must be classified as ‘Restricted and confidential’.  | **Storage**Secure in locked file cabinet, desk drawer or office.Do not leave unattended on monitor or desk when not in active use.Encryption or password protection required for storage on portable devices.**Destruction**[*State how these records should be destroyed, eg cross-shredding, placing in a designated locking disposal container, degaussing, or physical destruction of electronic media*]. |
| Confidential | Trade secrets and records containing non-public and/or proprietary company information.Personal information that is not otherwise classified as restricted, ie does not constitute personal data, eg anonymised **[**consumer OR **[**client**]]** lists.Records where disclosure will have a moderate impact for the business of data subject if disclosed.—[*insert example*]—[*—insert example*] | ‘Confidential’ or, as required:‘Confidential: do not forward, print or copy’‘Confidential: encryption required’‘Confidential: legal professional privilege’‘Confidential: without prejudice’‘Confidential: do not forward, print, or copy’‘Confidential: named recipients only’ | **Storage**Secure in locked file cabinet, desk drawer or office.Do not leave unattended on monitor or desk when not in active use.Encryption or password protection required for storage on portable devices.**Destruction**[*State how these records should be destroyed, eg cross-shredding, placing in a designated locking disposal container, degaussing, or physical destruction of electronic media*]. |
| General business records | Records containing non-confidential business information, eg—product information—business processes—marketing materials—routine correspondence—[*insert other*]—[*insert other*] | No specific requirements but, as required, you should consider:‘Internal use only’‘Do not transfer outside the company’ | **Storage** No specific requirements.**Destruction**Place paper records in recycling bin.Delete electronic records and backup copies. |
| Public | Records containing publicly available information**[**, unless that information contains data that is classified at a higher level (eg Personal Information /PII/SPII in public documents)**]**.—press release—published accounts/financial results—public website pages—annual report—[*insert other*]—[*insert other*]Low Business Impact if disclosed. | No specific requirements | **Storage** No specific requirements.**Destruction**Place paper records in recycling bin.Delete electronic records and backup copies. |

**Appendix 2**

**Records retention schedule**

**Data retention guidelines**

**Important note**

Please note that these are guidelines only, which set minimum retention periods for both physical files and electronically held data. If there is a genuine business need to retain data for a longer period, please contact the **[**board OR COLP OR data protection officer OR risk and compliance department**]**.

**Client files**

| Matter type | Retention period |
| --- | --- |
| Trust | End of trust period or date of vesting plus 6 yearsDocuments relevant to VAT liability—6 yearsTax papers—12 years after the end of the trust period |
| Deal files, including applications for finance and insurance products etc… | 6 years  |
| Matters on behalf of minors | 6 years from the date of the client attaining 18 years |
| All other client matter files | 6 years |
| [insert files types as required] |  |

**Anti-money-laundering and counter-terrorist financing records**

| Matter type | Retention period |
| --- | --- |
| Records, documents or information relating to an occasional transaction | 6 years from the date you know or have reasonable grounds to suspect the transaction is complete |
| Records, documents or information relating to:—any transaction occurring as part of a business relationship, or—CDD measures taken in connection with that relationship | 6 years from the date you know or have reasonable grounds to suspect the business relationship has come to an endSubject to a long-stop retention period of 10 years for records relating to each individual transaction |
| A copy of any documents and information obtained to satisfy CDD requirements, when your CDD is relied on by another relevant person | 6 years from the date on which you are relied on |

**Central business records**

| Record type | Retention period | Authority |
| --- | --- | --- |
| Accounts records | six years |  |
| Complaints records | one year from the conclusion of the complaint | A consumer may complain to the FCO within 6 months. It is therefore recommended that you retain records on complaints for at least one year after the complaint is closed, resolved or concluded. |

**HR records**

| Record type | Retention period |
| --- | --- |
| Accident books, reports and records | 3 years from the date of the last entry (if an accident relates to a child or young adult—until that person reaches 21 years) |
| Income tax and NI records and correspondence with HMRC | 3 years after the end of the financial year to which they relate |
| Retirement Benefits Schemes—notifiable events | 6 years from the end of the scheme year in which the event took place |
| Statutory Maternity Pay records | 3 years after the end of the tax year in which the maternity period ends |
| Statutory Sick Pay records | 3 years after the end of the tax year to which they relate |
| Salary and pay records | 6 years |
| Application forms and interview notes for unsuccessful candidates (the same data for successful candidates will be transferred to their Personnel files—see **Personnel files** below) | **[**6 months OR 1 year**]** |
| Parental leave records | 5 years from the birth or adoption of the child or 18 years if the child receives a disability allowance |
| Pension scheme investment policies | 12 years from the end of any benefit payable under the policy |
| Personnel files and training records (including disciplinary records and working time records) | 6 years after employment ceases |
| Redundancy records | 6 years from date of redundancy |
| Other HR records | **[**1 year OR 2 years**]** |