Howells

Retention and Destruction Policy

Contents

1 Purpose

This policy aims to set out the Company's stance on the appropriate retention and destruction of records containing personal data. It focuses on the personal data of members of staff. Where personal data belonging to any other data subject is handled in the Company, staff are encouraged to apply the principles of this policy, unless they have been instructed otherwise by an appropriate senior colleague.

It is also intended to be a key tool toward demonstrating compliance measures to regulators and may be regarded by them as a top layer document and therefore comprises part of our layered approach to documenting practices in this area.

2 Scope

2.1 As a UK established organisation, this policy applies to all our retention and destruction of personal data regardless of where in the world that processing may take place.

2.2 This is an internal policy and it applies to all employees, workers and any other internal persons who may have responsibility for the retention and deletion of documents or records containing personal data.

2.3 The policy should be read in conjunction with our General Data Protection Policy.

The document may be shared with third parties, contractors and other self-employed persons who will be asked to comply with the policy. Where the organisation undertakes the services of a third party, that party will be required to make adequate assurances to the data controller and/or processor their own processing is compliant with current applicable data protection laws.

2.4 This policy is not contractual but aims to set out how we normally deal with such issues.

3 Definitions

3.1 Anonymised

The identification of a data subject has been prevented irreversibly.

3.2 Generalised

Broad or non-specific information. Examples include: age ranges, salary bandings etc.

3.3 Recipient

A natural person or organisation to whom personal data is disclosed or made available to. A recipient is not necessarily a third party with who the Company has professional dealings.

3.4 Personal data (personal information)

Any 'data' relating to a 'data subject' who can be directly or indirectly identified by reference to a piece of data. This includes a name, identification number, location data or online identifier. It may be an identifier

that relates to physical, physiological, genetic, mental, economic, cultural or social identity. It may also apply to data that has been pseudonymised.

3.5 Pseudonymised

The direct identification of a data subject has been prevented.

4 Retention

4.1 Why we retain personal data

4.1.1 The Company only retains personal data it really needs. This data should always be relevant and necessary for a clear purpose.

4.1.2 Records are kept about members of staff for a broad range of processing activities. The most common categories include:

- Recruitment and right to work documentation
- Contact details
- Contracts, offers and variations
- Disciplinary and grievance
- Medical and occupational health
- Payroll information
- Performance
- Sickness and absence
- Any other job specific certifications eg criminal record checks, driving licences and insurance documents

4.1.3 We may also retain certain information in line with our IT Policy on monitoring. For example, where there is alleged misuse of Company working time, or misuse of company property, such as cars, equipment etc; we may review and retain any evidence of misuse.

4.1.4 The Company may retain some personal data for statistical purposes. These purposes may include analysis of employee turnover, career progression, remuneration and equal opportunities. It may include trend analysis of sickness absences, holidays and other types of leave.

4.2 Maintaining accuracy

4.2.1 All personal data retained by us must be accurate and where necessary kept up to date.

4.2.2 Members of staff are asked to keep the personal details we hold on them up to date. This includes any information that may change, such as: address, contact number, name etc. Any updates such as these should be provided without delay.

4.2.3 Every reasonable step to rectify or erase inaccurate or misleading personal data must be taken without delay.

4.2.4 When personal data is received from a source other than the member of staff (or data subject), reasonable steps should be taken to verify the authenticity of the source and the information. An example of this includes checking references are from a legitimate organisation.

4.2.5 When employment has ended for whatever reason, the personal data we may retain will no longer be kept up to date. However, the data will not be distorted in a manner that may be misrepresentative.

4.3 Confidentiality and integrity

4.3.1 Where feasible the personal data retained is generalised, pseudonymised or anonymised.

4.3.2 All personal data must be stored in a manner that ensures appropriate security of the personal data by using appropriate measures. At the very least, it must always be protected against unauthorised or unlawful access and processing, and against accidental loss, destruction or damage.

4.3.3 New methods of retention are assessed using a cost-benefit method. This is to ensure that any intrusion on privacy or potential adverse consequences of the methods are kept to a justified minimum.

4.3.4 The Company may record any inaccuracies that are updated, particularly in the event of an error. It may be necessary to understand the reason for the correction or to refer to the historical information. An example of this may include any minutes of meetings that are contested and amended due to differing recollections. In any event, the retention of the historical information will always be retained in a manner that is justified and does not mislead a recipient.

5 Destruction

5.1 When personal data should be removed

5.1.1 The Company prohibits a 'save-everything' approach purely for the sake of record keeping.

5.1.2 No personal data should ever be kept in a form which permits identification of a data subject for longer than is necessary to achieve the purpose for which it was collected.

5.1.3 As soon as there is no legal basis upon which the retention of personal data can be justified, it must be removed without delay.

5.1.4 Retention periods must always be kept to a minimum. Regard will be given to the needs of the business so that the proper running of the business, its interests and the management of staff shall not be significantly compromised.

5.1.5 Once employment ends regular access to a personnel file may no longer be required. Therefore, any documentation that should be retained post-employment is securely archived and access is restricted accordingly.

5.2 How personal data should be removed, returned, deleted or destroyed

Personal data is removed, deleted or destroyed as appropriate and in accordance with the 'Integrity and confidentiality' principle and 'Information security section' set out in the General Data Protection Policy.

5.2.1 When removing, returning, deleting or destroying any personal data, every reasonable and affordable step is taken to ensure it is done in a manner which is secure and ensures privacy; thereby keeping the risk of theft, loss or interception to an absolute minimum.

5.2.2 Appropriate and proper tools and processes must always be used.

5.2.3 If personal data can be anonymised, then where possible, identifying data must not be collected in the first place. If certain personal data is no longer required for the purpose and it becomes possible to anonymise data for any further purposes (e.g. reporting) then data is removed or deleted securely. Care must be taken to ensure that:

- Duplications are identified.
- Historical versions are identified (eg in computer history).
- Versions held in backup files or servers are identified.
- All identified versions that are no longer required are deleted securely and irrevocably.

5.2.4 If personal data can be pseudonymised, then care must be taken to ensure that:

- Duplications are identified.
- Historical versions are identified (eg in computer history).
- Versions held in backup files or servers are identified.
- Only a justifiable number of historical copies are retained and that any copies which may be deleted or removed are done so securely. Access to retained copies should be restricted to only those who absolutely require access at all times. Additional occasional access may be granted to others when and only for as long as access is required.

5.2.5 On instruction from the Controller, any personal data held on behalf of a client for whom we act as a processor, must be returned to the client without undue delay.

5.2.6 When returning or sending any personal data, it must be moved in a way which is secure and ensures privacy; such that the risk of theft, loss or interception is kept to a minimum. It must also be returned in a commonly used format. For example, HMRC returns will be via secure internet portal. Accounts will be via secure digital link. Emailing will be kept to a minimum. Reasonable steps should be taken to verify the identity of the recipient. For example, two forms of communication may be used such as making a telephone call to the recipient ahead of sending the information to a known e-mail address.

5.2.7 When deleting any personal data every effort must be made to identify any duplications of the data and to delete it securely. This includes historical versions and versions held in backup files or servers.

5.2.8 If it is necessary to destroy personal data or delete it irrevocably, then professional advice must be sought for example from an IT specialist. The must be notified of any intentions such as this in order to oversee the process.

5.2.9 If personal data is ever removed, deleted or destroyed accidentally or without authorisation of the Controller, it must be reported in accordance with the 'Breach and incident reporting' procedure.

5.2.10 On occasion it may be necessary to retain evidence of the removal, deletion or destruction of personal data, particularly when the data subject has requested information regarding the erasure or has asserted the right to be forgotten.

5.2.11 If we receive a request to have personal data erased or forgotten in accordance with a data subjects statutory right, then we may need to inform any recipients of that data so that the recipient may make steps to remove, return, delete or destroy the data as appropriate.

6 Set Retention Periods

6.1 Retention chart – explanatory notes

6.1.1 Figure 1 demonstrates the Company's usual retention periods for certain records relating to personnel.

6.1.2 Anyone who has responsibility for the maintenance and retention of these records is required to adhere to the retention periods listed.

6.1.3 The retention periods listed are the minimum length of time the record must be held for.

6.1.4 Many of the retention periods set out in figure 1 incorporate statutory requirements or professional practice rationales. Therefore, retention periods for these documents are mandatory.

6.1.5 Records should be removed at the point in time stated unless instructed otherwise.

6.1.6 In relation to Figure 1, any retention of records that exceeds the retention period stated must only be done so in an exceptional circumstance and where there is lawful justification. Authorisation must be sought from the Data Controller

6.2 Retention chart - figure 1

Document	Minimum Retention Period

Employee Relations	
Application forms and interview notes (for unsuccessful candidates)	6 months to a year
Applications (successful)	6 months following end of probation period – may retain useful data eg skills
Authorised absence records (annual leave, time of for dependents, jury service etc.)	2 years from when the entry was made
CCTV – relevant footage relating to an investigation or formal process	Extend normal retention period of CCTV for 6 months following a formal outcome or any appeal outcome
Collective agreements	6 years after ending
Contracts, offer letters and variations (including any flexible working outcome)	6 years following end of employment
Criminal record checks and disclosures (eg a DBS certificate)	6 years following end of employment
Capability and disciplinary documents (substantiated)	2 years following the issue of the warning
Driving licence (if required)	Duration drives on business plus 3 years
Driving offences	Remove once the conviction is 'spent' unless subject to exemptions.
Drug and alcohol testing records	6 years from a positive result 6 months from a negative result
Flexible working request documents	18 months following outcome (including any appeal outcome)
Grievance documents	6 months following end of employment
Investigations – no case to answer	6 months following conclusion
Maternity medical records	3 years after the end of the tax year in which the maternity period ends
Medical capability documents and records incl. OH reports	6 months following end of employment
Monitoring (eg vehicle trackers)	6 months rolling unless there is an overriding reason or on-going relevance of the record
Professional insurance (including insurance for driving on business), licence to practice and professional registrations.	6 years following end of employment
Qualifications	6 years following end of employment
Right to work checks	Two years after employment
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
Redundancy – documentation	6 years following end of redundancy

References received for employment	6 months following end of probation period
References issued for employment	1 year
References and correspondence that may produce legal affects (mortgage, loan, etc)	3 years following issue
Sickness records and unauthorised absence records	6 months following end of employment Pseudonymise where feasible
Sickness and injury records (work related) (other than those listed under 'Health and Safety')	15 years
Subject access request letters	1 year following completion of a request
Trust deeds, rules and minute books	Permanently
Whistle-blowing – reports and documents linked to an investigation which is partially or wholly substantiated.	6 months following the outcome of the report or any remedial action taken because of the report
Whistle-blowing – documents linked to an entirely unsubstantiated claim	Remove immediately any personal data
Health and Safety	
Accident books, records and reports	15 years
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Indefinitely
First aid training	6 years after employment
Fire warden training	6 years after employment
H&S representatives training	5 years after employment
H&S training - employees	5 years after employment
Health records made in connection with health surveillance (according to HSE)	40 years
Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos	Medical records - 40 years from the date of the last entry; Medical examination certificates - 4 years from the date of issue
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry if person is identifiable and the record represents exposure, otherwise at least 5 years.
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years

Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out
Risk assessments	Indefinite
Statutory and regulatory training	6 years after employment
Payroll and Finance	
Accounting records	3 years (private company) 6 years (public)
Expense accounts	6 years following year end (public companies)
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate
Inland Revenue/HMRC approvals	Permanently
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover
Statutory Maternity Pay records, calculations, certificates (Mat B1s) and leave	3 years after the end of the tax year in which the maternity period ends
Statutory Adoption Pay records, calculations, matching certificates and leave	3 years after the end of the tax year in which the maternity period ends
Statutory Paternity Pay records, calculations and leave	3 years after the end of the tax year in which the maternity period ends
Statutory Shared Parental Pay records, calculations, certificates (Mat B1s), notices and leave	3 years after the end of the tax year in which the maternity period ends
Wage/salary records (also overtime, bonuses, expenses)	6 years
Benefits	
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy however no information should ever be retained unless it is a necessary consequence of the funding
Pension records	12 years after benefit ceases. Avoid access unless required
Retirement Benefits Schemes – records of notifiable events	6 years from the end of the scheme year in which the event took place
Private medical	Avoid access unless required as part of making a reasonable adjustment etc
Working time	
Timesheets, overtime records and other documents relating to working time	2 years from date on which they were made
Young people and children	
Records relating to children and young adults	Until the child/young adult reaches the age of 21

7 Related policies and documents

- General data protection policy
- Breach and incident reporting procedure
- Disciplinary policy
- IT policy
- Recruitment and selection
- Whistleblowing policy

The above list is not exhaustive.

8 Further information

Any queries or comments about this policy should be addressed to Tracey Jackson

9 Policy owner

This policy is owned and maintained by Walter Howells Managing Director

10 Policy review date

Annually reviewed