

## **Introduction**

### *Purpose*

This policy largely concerns HR data and sets out our commitment to meeting our data protection obligations and to safeguarding our employees' rights and those of our clients in relation to their personal data that we process.

This policy applies to the personal data of employees during and after their employment with us.

The word "employee" is used throughout this policy but includes, where appropriate, workers, apprentices, interns, and volunteers.

The word "employment" is used throughout this policy but may include worker, contractor or volunteer relationships, or apprenticeships or internships.

It is data relating only to the company's HR activities. We term this data "HR personal data" and refer to in shorthand as HRPD.

Questions about our policy on data protection, or subject access requests, should be directed to the director.

The policy supplements the information already provided in our employee handbook and in the privacy notices sent to employees.

### *Terminology*

"**Personal data**" is any information that relates to a living individual who can be identified from that information.

"**Data Processing**" is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

"**Special categories of personal data**" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data. It was previously termed "sensitive data."

"**Criminal records data**" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

### ***Data protection principles***

We process HRPD in accordance with the data protection principles already well established in UK law. These are set out in full below.

- **Principle 1**

**Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:**

- a) at least one of the conditions in Schedule 2 of the Data Protection Act is met, and**
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Data Protection Act is also met.**

- **Principle 2**  
**Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.**
- **Principle 3**  
**Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.**
- **Principle 4**  
**Personal data shall be accurate and, where necessary, kept up to date.**
- **Principle 5**  
**Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.**
- **Principle 6**  
**Personal data shall be processed in accordance with the rights of data subjects under this Act.**
- **Principle 7**  
**Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**
- **Principle 8**  
**Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

We inform employees in our privacy notices, what data we hold; the reasons for processing that personal data; how we use such data and the legal basis for data processing. We will not process personal data of employees for any other reasons. Where we rely on our legitimate interests as the basis for processing data, we have carried out an assessment and believe that those interests are not overridden by the rights and freedoms of employees.

We have no need to process special categories of personal data in respect of clients' data save that which is held on our SAGE accounts in relation to invoicing. That is, the name of the accounts contact(s).

Employees' data are subject to additional safeguards.

Personal data gathered during employment are held in the individual's personnel file in hard copy or electronic format, or both, and on HR systems. The periods for which we hold HR-related personal data are contained in our privacy notices sent to employees or are in line with the appendix on document retention.

We keep a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

## **Individual rights**

As a data subject, employees have a number of rights in relation to their personal data.

### *Subject access requests*

Employees have the right to make a subject access request. If an individual makes a subject access request, we will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of that data if it has been provided by the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored;
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks we has failed to comply with his/her data protection rights; and
- whether or not We carries out automated decision-making and the logic involved in any such decision-making.

We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to Jack Jennings We will normally respond to a request within a period of one month from the date it is received.

If a subject access request is vexatious, manifestly unfounded, or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

If an employee submits such a request, we will notify him/her we consider this to be the case.

An employee may raise a grievance under the Company's procedure if he/she disagrees with our decision.

### *Other rights*

Employees have a number of other rights in relation to their personal data. They can require us to:

- make corrections to inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual withdraws consent;
- stop processing or erase data if processing is unlawful; and

- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override our legitimate grounds for processing data.

To ask us to take any of these steps, the individual should send the request to Jack Jennings.

### **Data security**

We take the security of HRPD seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by authorised employees in the course of their employment.

Where we share your personal data with third parties or engage them to process data on our behalf, such parties are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

### **Impact assessments**

We do not consider that any of the processing we carry out would result in a high risk to privacy such as to require us to conduct an impact assessment.

### **Data breaches**

If we discover that there has been a breach of HRPD that poses a risk to the rights and freedoms of Employees, we will report it to the Information Commissioner within 72 hours of discovery. All data breaches are recorded regardless of their effect.

### **International data transfers**

We do not transfer HR-related personal data to countries outside the EEA.

### **Individual responsibilities**

Employees are responsible for helping us keep their personal data up to date.

You should let us know if data provided to us changes, for example if you move house or changes bank details.

Employees who have access to the personal data of other employees and of our customers and clients in the course of their employment. Where this is the case, we require you to help us meet our data protection obligations.

Employees who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to employees who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

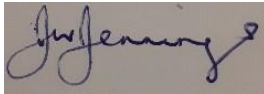
- not to remove personal data in any format from our premises without authority and then only in accordance with our rules or removing data
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to Jack Jennings immediately.

A failure to comply with the data protection rules associated with your employment would constitute a disciplinary offence and in cases where the breach has been flagrant and deliberate or a result of gross negligence, with potentially serious consequences for other employees or our customers, the penalty may be dismissal.

## **Training**

We provide training to all Employees commensurate with their data protection responsibilities.

**Signed**

A handwritten signature in black ink, appearing to read 'Jack Jennings', is written on a light-colored rectangular background.

**DATE 02 March 2023**

**Reviewed 19<sup>th</sup> February 2025**

## POLICY FOR THE RETENTION OF HR RECORDS

---

Our policy for the retention of HR records is based on guidance provided by the Chartered Institute of Personnel and Development (CIPD), a template for good business practice. By adopting the guidance, we aim to be compliant with the requirements of data protection legislation and employment law.

There are many different documents which can be described as HR or Personnel records. In some cases, there are statutory retention periods which must be complied with but in other cases the retention periods are advisory rather than being prescribed by law. In all cases we intend to manage this aspect of the business in line with the guidance issued by the CIPD and consequently that guidance is set out in full below.

### STATUTORY RETENTION PERIODS

---

The table below summarises the main legislation regulating statutory retention periods. However, it is a good idea to keep records for six years (five in Scotland), to cover the time limit for bringing any civil legal action.

Record	Statutory retention period	Statutory authority
accident books, accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).
accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
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	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676)

Record	Statutory retention period	Statutory authority
medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
<p>medical records under the Control of Asbestos at Work Regulations</p> <ul style="list-style-type: none"> <li>• medical records containing details of employees exposed to asbestos</li> <li>• medical examination certificates</li> </ul>	<ul style="list-style-type: none"> <li>• 40 years from the date of the last entry</li> <li>• 4 years from the date of issue</li> </ul>	The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/. 2739)
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	The Ionising Radiations Regulations 1999 (SI 1999/3232)
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	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
records relating to children and young adults	until the child/young adult reaches the age of 21	Limitation Act 1980
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

Record	Statutory retention period	Statutory authority
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894) as amended
wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
national minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
records relating to working time	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)



## RECOMMENDED (NON-STATUTORY) RETENTION PERIODS

For many types of personnel records, there is no definitive retention period: it is up to the employer to decide how long to keep these records.

Record	Recommended retention period
actuarial valuation reports	permanently
application forms and interview notes (for unsuccessful candidates)	6 months to a year. (Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants' documents will be transferred to the personnel file in any event.)
assessments under health and safety regulations and records of consultations with safety representatives and committees	permanently
Inland Revenue/HMRC approvals	permanently
money purchase details	6 years after transfer or value taken
parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
pension scheme investment policies	12 years from the ending of any benefit payable under the policy
pensioners' records	12 years after benefit ceases
personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases

Record	Recommended retention period
redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
senior executives' records (that is, those on a senior management team or their equivalents)	permanently for historical purposes
timecards	2 years after audit
trade union agreements	10 years after ceasing to be effective
trust deeds and rules	permanently
trustees' minute books	permanently
works council minutes	permanently