MURRAY & WILLIS

SPECIALIST REFURBISHMENT CONTRACTORS

# Data Protection Policy

# Contents

## 1. Purpose

To provide a procedure and a set of principles regarding the processing and protection of Personal Data contained within manual records and upon computer databases. It is also aimed at ensuring compliance with the General Data Protection Regulation (GDPR).

## 2. Scope

This Policy applies to all established and temporary employees who work under a contract of service and all other non-employed workers who work under a contract for service.
We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing any related policies and guidelines. That post is held by Dawn Clempson, HR and Training Manager. Please contact the DPO with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process Personal Data;
- if you need to rely on Consent;
- if you need to draft Privacy Notices;
- if you are unsure about the retention period for the Personal Data being Processed;
- if you are unsure about what security or other measures you need to implement to protect Personal Data;
- if there has been a Personal Data breach;
- if you are ever contemplating transferring Personal Data outside the EEA;
- if you need any assistance dealing with any rights invoked by a Data Subject;
- if you are engaging in a significant new, or change in, Processing activity which involves a high risk to the rights and freedoms of individuals and therefore may require a Data Protection Impact Assessment (DPIA);
- if you plan to use Personal Data for purposes others than what it was collected for;
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties.

## 3. Policy Statement

Murray and Willis Limited not only intends to comply with its obligations under the GDPR, but also wishes to assure both employees and all other persons about whom it retains personal data, that this will be processed in compliance with GDPR and will be stored in a secure, confidential and appropriate manner.

To this end, the Company is committed to upholding the following principles:

- personal data will be processed fairly and lawfully;

- the amount of personal data held will be adequate, relevant and not excessive in relation to the purposes for which it is held;
- personal data will be accurate and, where necessary, kept up to date;
- personal data will be obtained only for the specified and lawful purposes and will not be further processed in any manner incompatible with the purpose(s);
- personal data will only be held for so long as it is necessary to enable those specified and lawful purposes to be achieved;
- personal data will be secured against unauthorised or unlawful processing, accidental loss, destruction or damage;

## 4. Definitions

The following terms are used throughout this policy and its application:
"**Consent**" means agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

"**Data**" is information which is stored electronically, on a computer or in certain paper based filing systems:

"**Data Privacy Impact Assessment**" **(DPIA)**: tools and assessments used to identify and reduce risks of a data processing activity. A DPIA will be considered, in conjunction with the DPO, for any major system or business change programs involving the Processing of Personal Data.

"**Data Protection Officer**" **(DPO)**: the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means the person or team responsible for data protection compliance within the Company.

"**Personal Data**" is data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in possession of the data controller), including any expression of opinion about the individual and any indications of the intention of the data controller or any other person in respect of that individual.

"**Privacy Notices**" means separate notices setting out information that may be provided to Data Subjects when the Company collects information about them.

"**Sensitive Personal Data**" means personal data consisting of information as to racial or ethnic origins; political, religious or other opinions/beliefs of a similar nature; physical or mental health; sexual life; biometric or genetic data criminal offences or alleged criminal offences and past sentences; and whether he/she is a member of a trade union.

"**Data Controller**" means the people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the GDPR. The Company is the data controller of all personal data used in our business for our own commercial purposes.

"**Data Subject**" is an individual who is the subject of personal data.
"**Processing**" is obtaining, recording, holding or carrying out any operation on data; such as the organisation, adaptation, alteration, retrieval, disclosure, dissemination, rearranging or destruction of the information or the data.

"**Data Processor**" is any person who process data on behalf of the data controller (although employees of the Company are excluded from this definition).

## 5. Lawfulness and Fairness

The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

## 6. Notifying Data Subjects

The Company will only collect Personal Data when that information is required for a legitimate business or legal reason.

If we collect Personal Data directly from Data Subjects, we will inform them about their rights under the GDPR in a Privacy Notice which will include:

(a) The purpose or purposes for which we intend to process that personal data and the legal basis for the processing.
(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.
(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data including the right to object to processing.
(d) The right of subject access.
(e) The right to be forgotten.
(f) The right to withdraw consent, where processing is based on consent.
(g) The right to rectification if data is inaccurate or incomplete.
(h) Rights related to automated decision making and profiling.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

Most of the Personal Data we Process as part of our day to day operations will be that relating to our employees and sub-contractors. Please see Appendix I for the Privacy Notice relevant to the processing of data for all purposes relating to employment or engagement. The Privacy Notice will be made available to all potential sub-contractors and employees when they apply for work with the Company.

## 7. Specified, Explicit and Legitimate Purposes

In the course of our business, we may collect and process the personal data set out in Appendix II. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in Appendix II or for any other purposes specifically permitted by the GDPR. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

## 8. Data Minimisation

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

## 9. Retention Of Personal Data

9.1 Storage and Security

All documentation relating to employment or engagement is contained in hard copy, in an individual file for each person, within the Payroll department. Managers must not hold these or duplicate files locally.

The only exceptions to this principle are:

- Current Appraisal and objective/performance review documentation – which may be kept by the individual's line manager.
- Training and Development records – kept by the Human Resources and Training Manager.
- Health and Safety Assessments – kept by the Human Resources and Training Manager.

Hard copy records may not be removed from the department in which they are kept without the prior authorisation of the responsible manager named above.

The Company also stores and processes sensitive and other personal data electronically on the Payroll database. This system is managed and administered by members of the Payroll department. The Company also intends to store and process sensitive and other personal data electronically on a Human Resources database. This system is managed and administered by members of the Human Resources department.

The Company will take due care with regard to the storage of data and the protection of data, provided by software and hardware security measures. Every effort will also be taken to ensure the reliability and confidentiality of managers authorised as responsible for the maintenance of such information and training in the legal requirements and this policy will be provided to these managers.

If there is a data security breach which will result in a risk to the data subject we will report that

breach to the regulator without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

**Confidentiality** means that only people who are authorised to use the data can access it.

**Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

**Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

**Entry controls.** Any stranger seen in entry-controlled areas should be reported.

**Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

**Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required in line with our Disposal of Confidential Waste Policy.

**Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

9.2 Retention Period

The amount of data retained will be regularly reviewed and reduced so that only an appropriate amount is kept on record. We will not keep personal data any longer than is necessary for the purpose for which it was collected. The relevant departments will review all personal data each year in order to ensure that there are sound business or administrative reasons requiring the maintenance of that data. However, in order to meet legal requirements, it is necessary to retain employee information for a defined period after an employee has left the Company. The relevant time periods are shown in Appendix III.

9.3 Accuracy of Information

The Company will take such reasonable action as is necessary to ensure the accuracy of information. Data is deemed to be inaccurate if it is either incorrect or misleading as to any matter of fact.



The Payroll department will provide employees with a copy of the personal details held on the Payroll database, on a biannual basis, in order that they may update the data or raise queries regarding the content of the information. This will also apply to the data held on the Human Resources database.

In addition to the requirement for accuracy from a data protection perspective, information held is important for the correct administration of employee benefits and other details, such as telephone number and contact details of the next of kin, are also needed for Health and Safety reasons. For these and other employment reasons, it is a condition of employment that any change in an employee's circumstances must be notified by the individual to the Human Resources and Training Manager as soon as is practicable, so that records can be updated.

## 10. Processing In Line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller
- Object to processing, including in particular to prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.
- Obtain and reuse their personal data for their own purposes (where that right applies)

## 11. Access to Personal Data

All data subjects may request to see and have a copy of the sensitive and other personal data held by the Company:

Any data subject who is concerned as to the nature or existence of any personal data may request access to the personal data held by the Company by applying in writing to the Human Resources and Training Manager specifying the information that is requested. The Company will supply the information within 30 days of receiving a request but it should be noted that the original copy of the information held by the Company cannot be removed from its normal place of storage. Individuals will be accompanied by a member of the relevant department whilst viewing the information. The individual may also request a copy of the information for retention.

Similarly, managers may not remove the original copy of personal information held by the Company about their staff, from its normal place of storage, without the prior authorisation of the Human Resources and Training Manager and only after providing a written acknowledgement of the receipt of the information.

## 12. Personal Data Usage

All forms supplied by the Company to be completed by employees/workers or potential employees/workers for employment or engagement purposes will include an explanatory statement regarding the purpose for which the information is to be used, where the information will be kept and for

how long, and who will have access to the information.

Disclosure of information will only be permitted as referred to in this policy or if the individual has provided his/her consent.

Where the processing of data by automated means is likely to constitute the sole basis for any decision affecting the individual, such as is the case with certain psychometric tests, the individual will be informed of the logic involved in the decision making process.

Personal data will not be transferred to a country outside the European Economic Area without the individual/s consent to the transfer of the data.

## 13. References

Confidential references provided by the Company are exempt from the access provisions of the GDPR prior to their issue. This includes references supplied for the following purposes:

- education;
- training;
- employment;
- appointment to office;
- provision of any service.

This means that employees may not see a reference supplied by the Company before it is sent. However, the exemption is not applicable, and individuals may have access, to references once they are received by the Company and/or to references sent by the Company once they have been received by the intended third-party subject to a need to respect the privacy of the author of the reference.

The employee's permission for the Company to supply or obtain a reference must be obtained before any reference can be given or obtained. All persons voluntarily leaving the service of the Company will therefore be asked to confirm their agreement to such references being supplied to prospective future employers. Similarly, the written consent of an employee/worker must be provided before references will be supplied to Banks, Building Societies or other organisations. All potential workers will also be asked to provide their consent for the Company to obtain appropriate references for the completion of the security vetting process (as detailed in the Staff Screening Policy) at the time of their application to the Company.

All references relating to past and current employees must be written by a member of the Human Resources department, who will discuss the detail with the appropriate manager of the employee when necessary. Factual references will be supplied by the Company which confirm such details as length of service, position(s) held, reason for leaving, final salary and, if requested, attendance levels. Subjective statements will not be included within references supplied by the Company nor will telephone references be given.
Should a manager wish to provide a "character reference" for a past or current employee it must be explicitly stated that the reference is a personal reference from the individual concerned; it must not be sent on Company letter-head stationery and should not in any circumstances be considered to be the views or opinion of the Company.

## 14. Medical Records

For details of the right of access to any medical report prepared by a medical practitioner relating to employment the employee must either request details from the medical practitioner concerned or from the Human Resources and Training Manager. Details of employees' rights under the Medical Reports Act 1988 are specified prior to any employment medical being requested.
Any employee or any person authorised in writing by that employee may also apply to receive details of any health record obtained by the Company. Similarly, should the Company wish to apply for details of an employee's medical records retained by their general practitioner the employee's Consent will be requested before-hand.

## 15. Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.
Our staff may only share the Personal Data we hold with other staff if the recipient has a job-related need to know the information.
Our staff may only share the Personal Data we hold with third parties, such as our service providers, if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- where that third party is processing data on our behalf, a fully executed written contract that contains GDPR approved third party clauses has been obtained.

## 16. Amendments

Revisions, amendments or alterations to the policy can only be implemented following consideration and approval by the Managing Director.

## Appendix I Privacy Notice

**General Data Protection Regulation (GDPR)**

**Privacy Notice**

We issue this privacy notice in the interests of transparency over how we use ("**process**") the personal data that we collect from job applicants/employees ("**you**").

**Personal data** for these purposes means any information relating to an identified or identifiable person.

**"Sensitive personal data"** means personal data consisting of information as to -

a) the racial or ethnic origin of the individual,

b) their political opinions,

c) their religious or philosophical beliefs,

d) their membership of a trade union,

e) their physical or mental health or condition,

f) their sexual life,

g) the commission or alleged commission by them of any offence,

h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings,

i) genetic data; and

j) biometric data where processed to uniquely identify a person (for example a photo in an electronic passport)

**Data Controller**

For data protection purposes the "**data controller**" means the person or organisation who determines the purposes for which and the manner in which any personal data are processed.

The data controller is Murray & Willis Ltd, Units 4 & 5 Cannock Wood Industrial Estate, Cannock Wood Street, Rawnsley, Staffordshire WS12 0PL.

Our Data Protection Officer is Dawn Clempson, Human Resources & Training Manager who can be contacted on 01543 426 811.

**Purpose of processing the data**

It is necessary for us to process personal data of both job applicants and employees for the following reasons:

1. We will need the information in order to identify the individual for the purposes of recruitment;

2. We will need to maintain that information for the general purposes of the ongoing employment relationship including performing the employment contract and maintaining the health and safety of individuals on our premises.

Our legal basis for processing personal data of applicants and staff is that:

1. Processing the personal data is necessary for the purpose of carrying out the employment contract or to take steps to enter into an employment contract;

2. Processing is necessary to comply with a legal obligation (for example we are obliged under employment law to include in a written statement of employment terms the identity of the parties to the employment contract); and/or

3. Processing the data is necessary for the purposes of our "legitimate interests" as the data controller (except where such interests are overridden by the interests, rights or freedoms of the individual).

Our "legitimate interests" for these purposes are:

1. the need to process data on applicants and staff for the purposes of assessing suitability for employment and then carrying out the employment contract;

2. the need to gather data for the purposes safeguarding the health and safety of job applicants and employees;

3. the need to transfer employee data intra-group for administrative purposes; and

4. the need to process employee data for the purposes of ensuring network and information security.

We may from time to time need to process sensitive personal data, for example medical records or other information relating to the health and well being of an individual.

In that case we will either obtain the explicit consent of the individual to the processing of such data or we may consider the processing of that data as being necessary for carrying out our obligations as an employer. That will be assessed on a case by case basis.

There is no strict statutory or contractual requirement for you to provide data to us but if you do not provide at least that data that is necessary for us to assess suitability for employment and then to conduct the employment relationship then it will not practically be possible for us to employ you.

**Recipients of personal data**

Your personal data may be received by the following categories of people:

1. Our HR department;

2. In the case of job applicants, the interviewer and prospective manager;

3. Any individual authorised by us to maintain personnel files;

4. Our professional advisers; and

5. Appropriate external regulators and authorities (such as HMRC and HSE)

We do not envisage that your data would be transferred to a country outside the EEA. If we perceive the need to do that we would discuss that with you and explain the legal basis for the transfer of the data at that stage.

**Duration of storage of personal data**

We will keep personal data for no longer than is strictly necessary, having regard to the original purpose for which the data was processed. In some cases we will be legally obliged to keep your data for a set period. Examples are below:

Income tax and NI returns, income tax records and correspondence with HMRC: We are obliged to keep these records for not less than 3 years after the end of the financial year to which they relate.

Wage and salary records: We are obliged to keep these records for 6 years.

**Your rights in relation to your personal data**

1. The right to be forgotten

You have the right to request that your personal data is deleted if:

a) it is no longer necessary for us to store that data having regard to the purposes for which it was originally collected; or

b) in circumstances where we rely solely on your consent to process the data (and have no other legal basis for processing the data), you withdraw your consent to the data being processed; or

c) you object to the processing of the data for good reasons which are not overridden by another compelling reason for us to retain the data; or

d) the data was unlawfully processed; or

e) the data needs to be deleted to comply with a legal obligation.

However, we can refuse to comply with a request to delete your personal data where we process that data:

a) to exercise the right of freedom of expression and information;

b) to comply with a legal obligation or the performance of a public interest task or exercise of official authority;

c) for pubic health purposes in the public interest;

d) for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or

e) the exercise or defence of legal claims.

2. The right to data portability

You have the right to receive the personal data which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (us) where:

a) the processing is based on consent or on a contract; and

b) the processing is carried out by automated means.

Note that this right only applies if the processing is carried out by "automated means" which means it will not apply to most paper based data.

3. The right to withdraw consent

Where we process your personal data in reliance on your consent to that processing, you have the right to withdraw that consent at any time. You may do this in writing to the HR team or to your line manager.

4. The right to object to processing

Where we process your personal data for the performance of a legal task or in view of our legitimate interests you have the right to object on "grounds relating to your particular situation". If you wish to object to the processing of your personal data you should do so in writing to HR or to your line manager stating the reasons for your objection.

Where you exercise your right to object we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms; or

- the processing is for the establishment, exercise or defence of legal claims.

5. The right of subject access

So that you are aware of the personal data we hold on you, you have the right to request access to that data. This is sometimes referred to as making a "subject access request".

6. The right to rectification

If any of the personal data we hold on you is inaccurate or incomplete, you have the right to have any errors rectified.

Where we do not take action in response to a request for rectification you have the right to complain about that to the Information Commissioner's Office.

7. The right to restrict processing

In certain prescribed circumstances, such as where you have contested the accuracy of the personal data we hold on you, you have the right to block or suppress the further processing of your personal data.

8. Rights related to automated decision making and profiling

The GDPR defines "profiling" as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;
- location; or
- movement

You have the right not to be subject to a decision when it is based on automated processing; and it produces a legal effect or a similarly significant effect on you.

However, that right does not apply where the decision is necessary for purposes of the performance of a contract between you and us. We may use data related to your performance or attendance record to make a decision as to whether to take disciplinary action. We consider that to be necessary for the purposes of conducting the employment contract. In any event that is unlikely to be an automated decision in that action will not normally be taken without an appropriate manager discussing the matter with you first and then deciding whether the data reveals information such that formal action needs to be taken. In other words there will be "human intervention" for the purposes of the GDPR and you will have the chance to express your point of view, have the decision explained to you and an opportunity to challenge it.

**Complaints**

Where you take the view that your personal data are processed in a way that does not comply with the GDPR, you have a specific right to lodge a complaint with the relevant supervisory authority. The supervisory authority will then inform you of the progress and outcome of your complaint. The supervisory authority in the UK is the ICO.

## Appendix II Data Processing Activities

| Type of data | Type of data subject | Type of processing | Purpose of processing | Type of recipient to whom personal data is transferred | Retention period | Security Measures |
|---|---|---|---|---|---|---|
| Biometric Data – finger print data and individual photographs. | Employees, contractors of the Company and visitors | Collection, storage and recording on an electronic biometric time and attendance system | Maintenance of health and safety on site, e.g. fire evacuation; capturing attendance; performance of the contract with our client; training and timesheet calculation. The legal basis for the processing is set out in more detail in the Privacy Notice issued to the data subjects. | Donseed, who provide the system. | 40 Years as requested by the company insurance providers. | Controlled within the Company ISO 27001 procedures |
| CCTV Images | Employees and contractors of the Company and visitors | Collection, storage and recording on a CCTV system | Please see the Company's detailed CCTV Policy | | 30 Days | Rolling deletion of recordings;<br><br>Only accessed by authorised individuals.<br><br>Viewed only in restricted area.<br><br>For full details please refer to the Company's CCTV Policy |
| Basic staff information i.e. name, address, date of birth, telephone number | Employees and contractors | Collection, storage and recording on an electronic filing system | Necessary for the purposes of the employment contract | HR / Payroll / IT / HMRC / HSE / pension providers / Private Health | See Appendix III | Controlled within the Company ISO 27001 procedures |



| | | | | | | |
|---|---|---|---|---|---|---|
| Right to work documentation | | Collection, storage and recording on an electronic filing system | Necessary for the purposes of the employment contract | HR | See Appendix III | Controlled within the Company ISO 27001 procedures |
| Photographs of employees and contractors | Employees and contractors | Company Identification Cards<br><br>Website & Marketing<br><br>Company Newsletter | Access to sensitive client sites<br><br>Marketing Purposes<br><br>Information for Staff and Clients | Clients, potential clients and employees | Duration of engagement . | Controlled within the Company ISO 27001 procedures |
| Disciplinary records | Employee | Collection, storage and recording on an electronic filing system and Personel Files | Necessary for employment purposes | HR and Line Manager | See Appendix III | Controlled within the Company ISO 27001 procedures |
| Medical Information | Employees | Collection, storage and recording on an electronic filing system and Personel Files | Necessary for the purposes of the employment relationship – for example, complying with health and safety obligations and the duty to make reasonable adjustments | HR, H & S | See Appendix III | Controlled within the Company ISO 27001 procedures |
| Appraisals and performance reviews | Employees and contractors of the Company | Collection, storage and recording on an electronic filing system and Personel Files | To evaluate future training requirements and CPD | None | See Appendix III | Controlled within the Company ISO 27001 procedures |
| Client telephone numbers and addresses | Clients and prospects of the Company | Collection, storage and recording on an electronic filing system | To enable Murray & Willis to gain further work opportunities | None | Reviewed Annually | Controlled within the Company ISO 27001 procedures |

| | | | | | | |
|---|---|---|---|---|---|---|
| Payroll Records | Employees | Collection, storage and recording on an electronic filing system and Personel Files | To comply with the companies obligations to pay correctly and its legal obligations to HMRC | HMRC<br><br>Pension Providers<br><br>Auditors | See Appendix III | Restricted to Accounts and HR<br><br>Controlled under ISO 27001 procedures |
| Driving Licence | Employees and relevant contractors driving on behalf of the company | Licence Screening | To comply with Murray & Willis's legal obligation a nd its duty of care to employees | External Licence checking company and DVLA | Duration of employment (removed within 7 months of leaving) | Restricted to Accounts and HR<br><br>Controlled under ISO 27001 procedures |
| Screening Documentation | Employees and *Sub Contractors<br><br>*(Sub Contractors only if applicable to client contracts)* | Collection, storage and recording on an electronic filing system and personel file | Necessary to comply with the company screening policy – client requirement on various projects e.g. Financial Institutes | Sight of DBS disclosures may be requested by clients | Duration of employment (removed within 7 months of leaving) | Restricted to Finance Director and HR<br><br>Controlled under ISO 27001 procedures |
| Basic information i.e. name, address, telephone number, email address | Sub Contractors and Suppliers | Database | Approved sub contractor and supplier database for placing orders | Accountant, ISO Auditors for audit purposes only | Reviewed annually | Controlled under ISO 27001 procedures |
| Training Records | Employees, Sub Contractors and external training candidates | Database of training and scanned copies of certificates | To ensure Murray & Willis comply with its legal obligation under Health & Safety | Construction Industry Training Board (CITB) and clients if requested for proof of competence | 40 Years for all employees due to H & S compliance<br><br>External candidate<br><br>Date of expiry of training | Controlled under ISO 27001 procedures |

| | | | | | | |
|---|---|---|---|---|---|---|
| Site Inductions<br>Competency Questionnaires<br><br>Health Surveillance Risk Assessments | Employees and contractors | Collection and storage of site personnel information, competency questionnaire and Health Surveillance Risk Assessments | To ensure compliance with HSE legislation | H & S department<br><br>HSE<br><br>Insurance | 40 Years as requested by the company insurance providers. | Controlled within the Company ISO 27001 procedures |

## Appendix III Retention of Records

| SECTION AND CONTENT | RECOMMENDED RETENTION TIME |
|---|---|
| **Recruitment:**<br>Application Forms, CV's etc.<br>Interview Records and other selection records<br>References obtained<br>Proof of Right to Work in UK<br>Work Permits<br>Proof of Residence<br>Credit Check Services Report including Criminal Record Check | 7 months after employee has left employment |
| **Health & Safety/Medical :**<br>Tools/deductions from wages<br>Work wear and PPE<br>Sick notes | 6 years after employee has left employment |
| **Health & Safety/Medical :**<br>Health Assessments<br>Pre-employment medicals<br>Company Inductions | 40 years from time of assessment |
| **Terms and Conditions:**<br>Starter Form/Checklist<br>Offer letter<br>Statements of Terms and Conditions of Employment<br>Change to terms letters/documentation<br>Working Time Opt-Outs | 7 months after employee has left employment |
| **Payroll and Tax:**<br>P45<br>Tax Credits<br>Tax Code notification<br>Other personal tax or payroll documentation | 6 years after employee has left employment |
| **Employee Relations:**<br>Disciplinary records<br>Grievance records<br>Other formal performance reviews or attendance enquiries etc. | 7 months after employee has left employment |
| **General:**<br>Driving Licence<br>Fines<br>CICS details<br>Data Protection Consent Form<br>Other instructions and Authorisation | 7 months after employee has left employment |

Note that these are normal retention periods assuming there is no ongoing need to keep the documents at the end of that period. There may be cases where it is necessary to keep the documents for longer than the above periods. For example, if the employee is pursuing legal action against the Company and the records are necessary in order to defend the action.