

			<b>GDPR Records Management Notice</b>
Authorised: D Hulett		13 <sup>th</sup> March 2018	
Level 2 GDPR Policy	090-02-GDPR	Issue 3	
Last Revision: 10 <sup>th</sup> September 2019	Last Review: 31 <sup>st</sup> May 2018	Next Review: 31 <sup>st</sup> May 2019	

## Contents

1. DEFFINITIONS.....	2
2. INTRODUCTION.....	2
3. POLICY STATEMENT .....	3
4. MANAGEMENT OF RECORDS .....	4
4.1 STORAGE .....	4
4.2 ACCESS.....	4
4.3 INFORMATION AUDIT.....	4
4.4 DISPOSAL OF DATA.....	5
5. RETENTION SCHEDULE.....	5
6. REVISIONS .....	7

			<b>GDPR Records Management Notice</b>
Authorised: D Hulett		13 <sup>th</sup> March 2018	
Level 2 GDPR Policy	090-02-GDPR	Issue 3	
Last Revision: 10 <sup>th</sup> September 2019	Last Review: 31 <sup>st</sup> May 2018	Next Review: 31 <sup>st</sup> May 2019	

## 1. DEFFINITIONS

The GDPR Regulation	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
The Company	Any company in the John Lord Group of Companies
Us	John Lord Group of Companies
We	John Lord Group of Companies
Our	Belonging to John Lord Group of Companies
Data Subject	Any person whose personal data has been or is being processed by any company in the John Lord Group of Companies
Article	An article of The GDPR Regulation
Personal Data	Information which we hold and which uniquely identifies and is related to an individual person
Data Processing	Any operation or set of operations which is performed on personal data
Data Controller	The person or body who determines the purposes and means of data processing
Data Processor	Any person or body who processes personal data on behalf of the data controller

## 2. INTRODUCTION

- This policy outlines how records are stored, accessed, audited and disposed of.
- It also details the retention periods of different types of personal data.

			<b>GDPR Records Management Notice</b>
Authorised: D Hulett		13 <sup>th</sup> March 2018	
Level 2 GDPR Policy	090-02-GDPR	Issue 3	
Last Revision: 10 <sup>th</sup> September 2019	Last Review: 31 <sup>st</sup> May 2018	Next Review: 31 <sup>st</sup> May 2019	

### 3. POLICY STATEMENT

- Our company is committed to compliance with all elements of The GDPR Regulation as they affect us and will arrange our data record management in line with the principles set out in article 5 of The GDPR Regulation.
- Directors and senior management will ensure that the policies and procedures detailed in this policy document will be strictly implemented and will ensure that all employees and third party processors are made aware of and comply with these requirements.
- Our Privacy Officer is the first contact within our company with regards to data protection and the GDPR Regulation and can be contacted as follows: [privacy@john-lord.co.uk](mailto:privacy@john-lord.co.uk)

**Mark Hadfield**

**Managing Director John L Lord & Son (Rizistal)**

Signed:  Date: **31 May 2019**

**Martin Price**

**Managing Director Canal Engineering**


Signed:  Date: **31 May 2019**

**Tony Simpson**

**Managing Director SLS Design Consultants**

Signed:  Date: **31 May 2019**

**Review Date: 31 May 2020**

			<b>GDPR Records Management Notice</b>
Authorised: D Hulett		13 <sup>th</sup> March 2018	
Level 2 GDPR Policy	090-02-GDPR	Issue 3	
Last Revision: 10 <sup>th</sup> September 2019	Last Review: 31 <sup>st</sup> May 2018	Next Review: 31 <sup>st</sup> May 2019	

## 4. MANAGEMENT OF RECORDS

- Our company is committed to processing and safeguarding personal data in accordance with the following key principles:

### 4.1 STORAGE

- Personal data records will either be in hard copy format or electronic format depending on the type of record.
- Hard copies will generally be securely stored in folders dedicated to the data subject.
- Such folders are the responsibility of the specific data processor and will be locked away when the processor leaves the area.
- All hard copies of employee records are stored in a locked fire resistant cabinet in the admin office.
- We operate a “Clear Desk” policy throughout the company to avoid personal data being inadvertently disclosed to others who do not have a reason to view the data.
- Hard copies of personal data must not be removed from the premises.
- Electronic data will be stored in dedicated sections of our server and in personal email folders.
- Folder locations have restricted access and are password protected.
- Computers are password protected and encrypted.
- Personal data must not be stored on computer desktops, especially on laptop computers which are frequently removed from the premises.

### 4.2 ACCESS

- Personal data records may only be accessed by data processors that need to access them to perform their job as part of our legitimate business interest (LIA).
- Anyone believing they should have access to personal data which is currently restricted should initially consult the privacy officer.
- Data subjects should also contact the privacy officer to gain access to their records. The privacy officer will ensure that the data is only shared with the correctly identified data subject.

### 4.3 INFORMATION AUDIT

- We carry out annual information audits on all personal data held by the company to ensure that the data processing is necessary and is being correctly managed in accordance with The GDPR Regulation.
- The audits are carried out by the compliance department and will require the assistance of department heads when auditing specialist records and electronic applications.
- Information covered in the audit will include:
  - Hard copy documents and records
  - Electronic documents and records
  - Databases
  - Video records
  - Photographic records.

			<b>GDPR Records Management Notice</b>
Authorised: D Hulett		13 <sup>th</sup> March 2018	
Level 2 GDPR Policy	090-02-GDPR	Issue 3	
Last Revision: 10 <sup>th</sup> September 2019	Last Review: 31 <sup>st</sup> May 2018	Next Review: 31 <sup>st</sup> May 2019	




- The audits will be carried out in line with other company audits as described in [the Internal Audit and Review Procedure](#)
- Audit reports will be acted upon as described in the above procedure and will be included in the annual Management Review

#### 4.4 DISPOSAL OF DATA

- All personal data listed on the retention schedule below will be permanently disposed of at the end of the retention period.
- Hard copies of personal data will be shredded.
- Electronic personal data will be removed by the external IT provider to ensure that the data is non-recoverable.
- The privacy officer maintains the Data Deletion Record, which is a record of data that has been destroyed including details of who authorised the destruction and who carried out the destruction.

## 5. RETENTION SCHEDULE

DATA DESCRIPTION	RETENTION PERIOD
<b>EMPLOYEES</b>	
Job applications and interview records of successful candidates	6 years after employment ceases
Job applications and interview records of unsuccessful candidates	6 months after notifying unsuccessful candidates, unless the company has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained.
Emergency contact details	Destroyed on termination
Right to work in the UK documentation, including copies of passport and certificates such as birth certificates	2 years after employment ceases
Contracts of employment and changes to terms and conditions	6 years after employment ceases
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.
Personnel and training records	While employment continues and up to 10 years after employment ceases

			<b>GDPR Records Management Notice</b>
Authorised: D Hulett		13 <sup>th</sup> March 2018	
Level 2 GDPR Policy	090-02-GDPR	Issue 3	
Last Revision: 10 <sup>th</sup> September 2019	Last Review: 31 <sup>st</sup> May 2018	Next Review: 31 <sup>st</sup> May 2019	

Disciplinary records	6 years after employment ceases
Immigration checks	2 years after employment ceases
Health Surveillance Records	40 years after employment ceases
Working time regulation opt-out records	2 years after employment ceases
Annual leave records	6 years after the end of tax year they relate to.
Absence records	6 years after employment ceases
Maternity / paternity / adoption leave records	3 years after the end of tax year they relate to.
Statutory sick pay records	3 years after the end of tax year they relate to.
<b>FINANCIAL</b>	
Pension records	12 years after employment ceases
Payroll records including time sheets	6 years after employment ceases
PAYE Records	6 years after employment ceases
Employee bank details	Destroyed on final payment
Annual accounts	6 years after the end of tax year they relate to.
Individual budgets	Duration of the budget plus 3 years
<b>HEALTH AND SAFETY</b>	
Accident records	10 years after employment ceases
HSE RIDDOR reports	12 years after employment ceases
Visitors book	6 years
Method statements	10 years from end of contract
Fire Log book	6 years
Air monitoring records	10 years after employment ceases
<b>CONTRACT MANAGEMENT</b>	
All client contract records	12 years from end of contract

			<b>GDPR Records Management Notice</b>
Authorised: D Hulett		13 <sup>th</sup> March 2018	
Level 2 GDPR Policy	090-02-GDPR	Issue 3	
Last Revision: 10 <sup>th</sup> September 2019	Last Review: 31 <sup>st</sup> May 2018	Next Review: 31 <sup>st</sup> May 2019	

## 6. REVISIONS

Date	Pages / Sections	Issue Status	Amendment Details
13 <sup>th</sup> Mar 2018	All	Issue 1	First issue of Policy
31 <sup>st</sup> May 2019	All	Issue 2	Annual Policy Review – no revisions
10 <sup>th</sup> September 2019	All	Issue 3	Revised numbering format