GDPR Compliance Statement

What is the GDPR

The EU General Data Protection Regulation ("GDPR") came into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

1. LLWRs Commitment

LLWR are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

LLWR are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

LLWR already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR. Our preparation has included: -

- ***Information Audit*** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed. This is captured in the departmental Data Resource Spreadsheet for each area.
- ***Policies & Procedures -*** revising data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:
    - ***Data Protection*** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities.
    - ***Data Retention & Erasure*** – we are reviewing our retention policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.

- ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time in line with ICO guidance
- ***International Data Transfers & Third-Party Disclosures*** –LLWR does not store or transfers personal information outside the EU, however for UK based organisations we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

Subject Access Request (SAR) – An employee has the right to access information kept about them by LLWR LTD, including but not limited to: personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee. The HR Department is responsible for dealing with data subject access requests. We promise to accommodate the revised 30-day timeframe for providing the requested information, subject to the correct circumstances and are aware of the circumstances when we can extend the time limit to respond to a request. We also understand when to consider if a request includes information regarding others and any implications this may have.

- ***Legal Basis for Processing*** - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met. See below for a summary of processing activities:

Department	***Purpose***	***Category of individuals***	***Category of personal data***
Human Resources	*Staff administration, fulfilment of contractual obligation, succession planning and staffing, correspondence to employees, legal compliance, monitoring information,*	*Employee data*	*Names, addresses, salary, bank details, pension details, occupational health details, case management, pension documentation, performance and rewards paper work, bonus information, sickness figures*
Duty Management team	*Fulfil the duty manager role*	*Employee data*	*Names, addresses, contact details*
IS&T	*Compliance with software licensing and organisational RSGs and to monitor usage of organisation assets and WIFI, updating of the directory, Cyber security monitoring*	*Employee data*	*Name, log in details, assets assigned, names, locations, contact details*
Project controls	*Implementing timesheet procedure, allocating costs*	*Employee data*	*Name, resource number, tariff rate, contact details.*

GDPR Compliance Statement

Department	***Purpose***	***Category of individuals***	***Category of personal data***
Commercial and contract management	*Compliance with legal and contractual obligations in case of potential claim or legal dispute.*	*Employee and stakeholders*	*Names, addresses, contact numbers, legal access documents*
National waste programme	*Contractual fulfilment with suppliers, training compliance*	*Employees and Suppliers/ stakeholders*	*Names, contact details, email addresses, CVs, training records*
Contractor validation	*Compliance with organisational RSGs for external visitors, short term workers and contractors*	*Contractor/sub-contractor*	*Names, addresses, contact details, training records, pass applications*
Waste Management Services	*Contractual agreements, compliance with organizational policy and transport legislation, LLWR T&S policy*	*Contracted suppliers/ haulers, employees*	*Names, addresses, contact details (employees) Supplier details, driver name and licence details*
Training	*Site licence condition compliance, SQEP evidence, compliance with organisational RSPs, succession planning, training attendance evidence*	*Employees Contractors*	*Names, resource ID, contact details.*
Science and Engineering	*Training records for compliance*	*Employees contractors*	*Name, resource ID, contact details.*
Security	*Compliance with clearance process and Nuclear Safety procedures*	*Employees Contractors*	*Names, addresses, NI number, contact details, previous employees/ references, photographic ID, CCTV recording*
Radiological protection	*Compliance with HSE and organisational policy*	*Employees Contractors*	*Medical records, names, resource ID, contact details*
Finance	*Payroll activities*	*Employees ASWs*	*Name, bank details, address, tax codes, pension data (employee) Name, resource ID (ASW)*
Generic line management	*To fulfil line manager responsibilities*	*Staff, ASW, CSW, Contractor*	*Names, contact details, performance paperwork (staff only), ASW scope and rate of pay, training records, sickness absence*

- ***Privacy Notice/Policy*** – we are revising our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

- ***Obtaining Consent*** – we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- ***Direct Marketing*** – LLWR do not provide any direct marketing.
- ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we are revising our documentation processes that record each assessment, this will allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment, hosting etc.*), every care has been taken to ensure all parties are compliant with the GDPR and are aligned to LLWR's ongoing commitment. These measures have included initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- ***Special Categories Data -*** Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, or is provided directly by an employee with the right to modify or remove consent being clearly signposted.

2. Correction of data

LLWR LTD has a system in place that enables employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an employee becomes aware that LLWR LTD holds any inaccurate, irrelevant or out-of-date information about them, they must notify the HR department immediately and provide any necessary corrections and/or updates to the information. The individual can also amend certain personal information themselves within People Management System. Aside from this annual information checks and workforce correspondence reviews are conducted regularly to assess the accuracy of the data held.

3. Monitoring

LLWR LTD may monitor employees by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, LLWR LTD will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about him/her. LLWR LTD will not retain such data for any longer than is necessary.

In exceptional circumstances, LLWR LTD may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to LLWR LTD by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means (for example, where an employee is suspected of stealing property

belonging to LLWR LTD). Covert monitoring will take place only with the approval of the Managing Director and Head of HR & Training.

4. Employees' Obligations Regarding Personal Information

Employees whom handle person data must ensure that:

- The information is accurate and up to date, insofar as it is practicable to do so;
- The use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- The information is secure.
- Uses password-protected and encrypted software for the transmission and receipt of emails;
- Sends fax transmissions to a direct fax where possible and with a secure cover sheet; and
- Locks files in a secure cabinet.

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded.

Where an employee is required to disclose personal data to any other country, they must ensure first that there are adequate safeguards for the protection of data in the host country.

An employee must not take any personal information away from LLWR LTD's premises without the prior consent of the Head of HR & Training.

If an employee is in any doubt about what about what they may or may not do with personal information, they should seek advice from the HR Department

5. Consequences of Non-Compliance

All employees are under an obligation to ensure that they comply with the data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this document may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal.

6. Taking Employment Records off Site

An employee may take only certain employment records off site. These are documents relating to [disciplinary or grievance meetings that cannot be held on site/meetings with occupational health/discussions surrounding the sale of the business or specific monitoring purposes/seeking professional advice]. Prior authorisation must
be sought from the Head of HR and Training.

Any employee taking records off site must ensure that they do not leave their laptop, other device or any hard copies of employment records unattended. They must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

GDPR Compliance Statement

7. Loss of Data

LLWR takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- Restricted access to files and folders, with a view of all personal data is accessed on a 'need to know' basis
- Encryption software for sending personal data/special personal data
- Explicit guidance regarding the security marking of such previously mentioned data
- An appointed CISO (Chief Information Security Officer) to review LLWR compliance and best practice surrounding all aspects of cyber security
- Accountable for reporting any breaches to the SIRO (Senior Information Risk Owner)

However, should there be any incident occur where there is loss or potential loss of personal or special personal data, it should be reported to the LLWR Data Controller immediately. If the Data Controller is unavailable, then the Deputy Data Controller should be sought and RSG 18.03_30 followed.

8. Compliance

General Data Protection Regulation	2018
Data Protection Act	1998

9. Definitions/Abbreviations

GDPR	General Data Protection Regulation
ICO	Information Commissioners Office
LLWR	Low Level Waste Repository
RSG	Repository Site Guidance

10. Supporting Information

RSG 18.03_30 - Reporting Personal Data Loss

11. Amendment Record

Issue 0 to Issue 1

Date	Section / Paragraph Amended	Amendment Details
March 2019	Whole document	First issue