DATA SECURITY, PROTECTION AND CONFIDENTIALITY (INCLUDING INTELLECTUAL PROPERTY)

Policy Statement

Riverside Environmental Services Limited holds personal and confidential information about its employees, customers, board members, employment applicants and suppliers. All individuals have a right to privacy and the company is bound by the Data Protection Act 1998 and GDPR

This policy is concerned with the storage, processing and accessibility of all personal information held by Riverside Environmental Services. It outlines the position of the company with regard to the nature of data to be held, the fair and lawful processing of such data, and deals with issues relating to the confidentiality of information and its availability to our customers.

The company welcomes the objectives of Data Protection legislation, recognising that personal information is confidential and that unauthorised disclosure may constitute a breach of contract and an offence under the Data Protection Act and GDPR.

T . 0870 950 0161
F . 0870 950 0162
E . info@riverside-es.com

riverside-es.com

Riverside Environmental Services Ltd
Unit 12 Whiffens Farm
Clement Street
Hextable
Kent BR8 7PQ

Midlands Office
Zone C Stargate Business Centre
Faraday Drive
Bridgnorth
Shropshire WV15 5BA

UKAS TESTING 4087
UKAS INSPECTION 0296

Company Registration No. 4620034

RESL have appropriate procedures in place to protect the security of client and employee data and to ensure personal data breaches are detected, reported and investigated effectively.
RESL will hold data in accordance with our Data Retention Policy. We will only hold data for as long as necessary for the purposes for which we collected it.

RESL is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

The aims of this policy are as follows:

- to ensure that the company complies with the legal requirements set out by the Data Protection Act 1998 – GDPR and other relevant legislation;
- to set out the principles of the company's approach to data privacy and protection;
- to outline the rights of customers with regard to access to information, and their entitlement to confidentiality;
- to specify responsibilities for ensuring compliance with the policy.

Guiding Principles

In adopting this Policy, Riverside Environmental Services is guided by the following broad Data Protection principles:

- personal data shall be processed fairly, lawfully and transparently;
- personal data shall be obtained only for one or more specified and lawful purposes, as set out in the company's registration entry with the Information Commissioner, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- personal data shall be accurate and, where necessary, kept up-to-date;
- personal data processed for any purpose shall not be kept for longer than is necessary for that purpose;
- personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998 and GDPR;
- 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.

In addition to these, Riverside Environmental Services shall also recognise the following:

- individuals have the right to access information that the company holds on them subject to certain exceptions permitted by law
- You have the right to information about what personal data we process, how and on what basis as set out in this policy.

- You have the right to access your own personal data by way of a subject access request (see above).
- You can correct any inaccuracies in your personal data. To do you should contact our Data protection Officer (DPO).
- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact our DPO
- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact our DPO
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to object if we process your personal data for the purposes of direct marketing.
- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, you have the right not to be subjected to automated decision-making.
- You have the right to be notified of a data security breach concerning your personal data.
- In most situations we will rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact our DPO.
- You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.
- individuals have the right to expect that the company shall keep such personal information confidential, unless specific circumstances apply that determine this would be inappropriate. These specific circumstances shall be defined within the "Access to Personal Information Policy".

Individual Data Subjects: Information Access

Individuals may request a copy of information held about them by Riverside Environmental Services and can seek its amendment/erasure if this is inaccurate or no longer required. The procedure for dealing with such requests is set out in the "Access to Personal Information Policy".

Duties of Employees and Board Members

It is the responsibility of all employees and Board Members to maintain confidentiality as set out within this policy. A breach of confidentiality is a serious offence.

You will receive appropriate training on the provisions and implementation of Data Protection Legislation.
It is your responsibility to inform a senior manager when you are made aware of a breach of confidentiality. The senior manager is then responsible for taking appropriate action when he/she is made aware of such a breach.

Disclosure of Information

Information on individuals is considered to be confidential, and will only be passed to other organisations with the express written consent of the individual concerned, unless there are exceptional circumstances. Such circumstances include:

- where there is clear evidence of fraud
- to comply with the law
- in connection with legal proceedings
- where it is essential and lawful to enable the company or other agencies with which the company co-operates to carry out their duties.

Requests from third parties for such access shall only be considered where these are made in accordance with the process specified in the "Access to Personal Information Policy".

Personal data breaches

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

A personal data breach means a breach of security leading to the accidental, unlawful or deliberate:

- Destruction;

- Loss;
- Alteration;
- Unauthorised disclosure of; or
- Access to personal data.

A breach is more than just about losing data.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*"

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Reporting a Breach

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

The types of breaches that require reporting to the ICO are:

- Breach of the Data Protection Act (DPA);

- A privacy and electronic communications (PECR) security breach by a telecoms or Internet service provider; or
- The unlawful obtaining of personal data (known as a Section 55 DPA breach).

The ICO website at www.ico.org.uk\for-organisations\report-a-breach contains the necessary link and forms for reporting such breaches.

www.ico.org.uk\for-organisations\improveyourpractices

If there is a breach, the DPO and board member should be advised. Either or both will then determine what type of breach has occurred and what requires reporting to the ICO.

Confidentiality – Employees' Responsibilities

You will not disclose, either during or after the termination of your employment, any information of a confidential nature relating to the company, its customers or suppliers or any third party which may have been obtained in the course of this employment without first obtaining the written permission of the Managing Director. This does not apply where such information is in the public domain otherwise than by your default.
You will not make any public statement or any statement to a person employed or associated with the media concerning the company, its customers or suppliers or their activities without first obtaining the written permission of your manager.

You will not place yourself in a position in which your interests conflict with those of the company.

Intellectual Property and Patents

It will be part of your duties, as an employee of Riverside Environmental Services, to consider how the products, services, processes, equipment or systems of the company might be improved promoted and marketed. Any invention, development, process, plan, design, formula, specification, programme or other matter whatsoever (collectively known hereafter as 'the Inventions') made, developed or discovered by you, either alone or in concert, whilst you are employed by the company shall forthwith be disclosed to the company and, subject to Section 39 of the Patents Act 1977 and any succeeding statutory provision, shall belong to and be the absolute property of the company or such subsidiary as it may designate.

The company shall decide, in its sole discretion, whether and when to apply for patent, registered design or other protection in respect of the Inventions and reserves the right to work any of the Inventions as a secret process, in which event you shall observe the obligations relating to confidential information which are contained in your contract of employment.

Any patent rights expected as a result of work undertaken by you as part of your work are the property of the company.

The copyright in any material produced by you relating to your employment with the company rests with the company. You undertake to provide Riverside Environmental Services with every assistance in protecting the company's intellectual property rights.

Monitoring and Responsibilities

It is the responsibility of the Managing Director to ensure that implementation of the Data Security - Protection and Confidentiality Policy (including Intellectual Property) is monitored.

Riverside Environmental Services shall ensure that it has a named Data Controller, who will offer advice to employees, Board Members and customers on the implementation of this Policy.

The capture, availability, processing, and purging of personal data shall comply with company policies and all appropriate legislation, and will be monitored and managed by the Data Controller.

A review of the effectiveness of this policy will be undertaken by the Data Controller every year and a report summarising the findings of this review will be submitted to the Board.