Data Protection Policy Statement

Policy, Scope and Objectives

The Directors and management of Simer Environmental Services Ltd are committed to compliance with all relevant UK and EU law in respect of personal data. We are dedicated to protecting the personal data of information collected from individuals in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act.

Notification

We have identified all the personal data that we process, and this is contained in our Information Audit, this is periodically reviewed to ensure it reflects any technological or organisational changes.

This policy applies to all Employees/Staff and interested parties of Simer Environmental Solutions Ltd such as outsourced suppliers. Any breach of the GDPR will be dealt with under our disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for Simer Environmental Services Ltd, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Simer Environmental Solutions Ltd without having first entered into a data confidentiality/GDPR agreement which imposes on the third-party obligations no less onerous than those to which Simer Environmental Services Ltd is committed, and which gives Simer Environmental Services Ltd the right to audit compliance with the agreement.

Definitions used by the organisation (drawn from the GDPR)

- **Personal data** - Personal data" is any information that relates to an individual who can be identified from that information.
- **Data controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Data subject** – any living individual who is the subject of personal data held by an organisation.
- **Personal data breach –** a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.
- **Data subject consent –** means any freely given, specific, informed and unmistakable indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Responsibilities under the General Data Protection Regulation

Simer Environmental Services Ltd is a data controller and data processor. Top Management and all those in managerial or supervisory roles throughout Simer Environmental Services Ltd are responsible

for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions and within the organisational structure.

Our Director is responsible for ensuring that compliance with data protection legislation and good practice can be demonstrated. Managers and Directors have responsibilities for ensuring data processing takes place appropriately within their area of responsibility. However, compliance with data protection legislation is the responsibility of all members of Simer Environmental Solutions Ltd who process personal information.

Additionally employees and contractors are responsible for ensuring that any of their personal data supplied by them to Simer Environmental Services Ltd, is accurate and up-to-date.

Risk Assessment

We have a robust risk assessment process to ensure that Simer Environmental Services Ltd is aware of any risks associated with the processing of particular types of personal information. This assesses the level of risk to individuals associated with the processing of their personal information. Where necessary, assessments will also be carried out in relation to processing undertaken by other organisations on behalf of Simer Environmental Solutions Ltd.

Simer Environmental Services Ltd shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy. Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level and meet requirements of regulations.

We aim to adopt a privacy by design approach and will carry out a Privacy Impact Assessment (PIA), also referred to as 'Data Protection Impact Assessments' (DPIA), as part of our GDPR compliance system in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and we cannot sufficiently address those risks, we will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Data protection principles

All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and our policies and procedures are designed to ensure compliance with them.

- **Personal data must be processed lawfully, fairly and transparently.**

Simer Environmental Solutions Ltd Fair Processing Procedure is set out in our GDPR manual

- **Personal data can only be collected for specified, explicit and legitimate purposes.**

Data obtained for specified purposes must not be used for a purpose that differs from those defined in our privacy notice and GDPR manual.

- **Personal data must be adequate, relevant and limited to what is necessary for processing.**

We will ensure that, on an annual basis all data collection methods are reviewed by to ensure that collected data continues to be adequate, relevant and not excessive. Director will review all the

personal data maintained by Simer Environmental Services Ltd, by reference to the Information audit, and will identify any data that is no longer required will be securely deleted/destroyed.

If data is given or obtained that is excessive or not specifically required by Simer Environmental Solutions Ltd's documented procedures, Director is responsible for ensuring that it is securely deleted or destroyed.

- **Personal data must be accurate and kept up to date.**

Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

Staff are trained in the importance of collecting accurate data and maintaining it. It is also the responsibility of individuals to ensure that the data that they provide held by Simer Environmental Solutions Ltd is accurate and up-to-date. They should notify us of any changes in circumstance to enable personal records to be updated accordingly.

Instructions for updating records are contained Documented information Procedure BP12. It is the responsibility of Simer Environmental Services Ltd to ensure that any notification regarding change of circumstances is noted and acted upon, this includes informing any third party data processor as necessary.

- **Personal data must be kept in a form such that the data subject can be identified only if is necessary for processing.**

Where personal data is retained beyond the processing date, it will be minimised in order to protect the identity of the data subject in the event of a data breach. Personal data will be retained in line with the Documented Information procedure BP12 and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

Director must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

- **Personal data must be processed in a manner that ensures its security**

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. These controls have been selected based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data. The transfer of personal data outside of the EU is prohibited unless safeguards or exceptions apply as specified within GDPR.

- **Accountability**

GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

- **Data subjects' rights**

Data subjects have the following rights regarding data processing, and the data that is recorded about

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- The right to object to any automated profiling without consent.

Data subjects may make data access requests, our GDPR manual describes how Simer Environmental Services Ltd will ensure that its response to the data access request complies with the requirements of the Regulation.

Complaints

Data Subjects who wish to complain to Simer Environmental Solutions Ltd about how their personal information has been processed may lodge their complaint directly with the Director, who will investigate and respond accordingly within one month. Complaints should be sent addressed to:
Director, Simer Environmental Solutions Ltd
15 Arnside Rd, Waterlooville PO7 7UP

Our Privacy Notice communicates this publicly.

Should the response not be resolved to the satisfaction of the complainant, the individual can also take up their issue with the Information Commissioner's Office (the ICO) at the following address:
The Information Commissioner's Office, Wycliffe House, Water Ln, Wilmslow SK9 5AF

Consent

Simer Environmental Services Ltd understands 'consent' to mean that it has been explicitly and freely given, specific, and informed indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time. There will be limited circumstances when consent will be the relevant legal basis for processing of personal data by Simer Environmental Solutions Ltd.

Should consent be the relevant legal basis to process personal and sensitive data it will obtained using standard consent documents.

Security of data

All Employees/Staff are responsible for ensuring that any personal data which Simer Environmental Services Ltd holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorized by Director to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected
- stored on (removable) computer media which are encrypted

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Simer Environmental Services Ltd.

Manual records containing personal data may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorization from Director. As soon as manual records are no longer required for day-to-day client support, they must be removed for secure archiving

Personal data may only be deleted or disposed of in line with Documented Information Procedures. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately securely destroyed.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held by Simer Environmental Solutions Ltd in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by Simer Environmental Services Ltd, and information obtained from third-party organisations about that person.

Subject Access Requests are dealt with as described in GDPR Manual.

Disclosure of data

Simer Environmental Services Ltd must ensure that personal data is not disclosed to unauthorised third parties. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Simer Environmental Solutions Ltd's business.

The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by Director.

Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left Simer Environmental Solutions Ltd, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. Simer Environmental Services Ltd's Documented Information Procedure will apply in all cases.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) to ensure secure disposal.

Simer Environmental Services Limited is registered with the Information Commissioners Office as a data controller, registration number ZA757496

M. Wood
Director
April 2023