Data Protection Policy

V1.1 August 2024

Our purpose

To create a **healthier**, **safer**, and more **beautiful** world

Our mission

To be the market leader and trusted partner for clients.

Our values

DATA PROTECTION POLICY

Associated Group Policies:	Acceptable Use Policy Privacy Policy	**IMS Reference:**	HR0012
Department:	HR/IT	**Review date:**	August 2024
		Next review date	August 2025

Revision	Date	Revision Description	Requested by
V 1.0	February 2023	New policy and procedure	Eoin O'Connell - CIO
V 1.1	August 2024	Annual review, changed Rokill to Nurture Pests and added scope statement.	Yogesh Agarwal - DPO

	Author:	Owner:	Approver:
Name:	RightCue	Nurture Group	Gareth Kirkwood
Job Title:	Ex Consultants	DPO	CEO

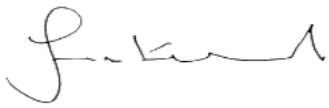
CEO Signature: 

Table of Contents

Glossary of Terms

Term / Acronym	Definition / Meaning
Nurture Group	Nurture Group including Nurture Group Landscapes Limited, Gavin Jones Limited, Nurture Pests Limited.

1 Purpose

This Policy sets out the obligations of Nurture Group regarding data protection and the rights of the individuals (in this context, "data subjects") in respect of their personal data under the UK Data Protection Legislation.

It should be considered alongside more detailed information security documentation, including, Annexures to this policy, information security policy and related ISMS documentation, security guidance and protocols or procedures.

Nurture Group receives and processes personal data in respect of its customers, prospects, suppliers, employment candidates, employees, and other contacts.

In addition, the Group may receive and process personal information on behalf of its customers (acting as data processor). All such information is subject to any data protection requirements, in addition to this Policy, that may have been agreed upon with the customers.

References in this policy to "we", "our", and "us" shall be a reference to the Nurture Group, which includes the Group Holding Company, group companies, affiliated companies, associates, and non-incorporated bodies that are considered part of the Nurture Group.

2 Scope

This Group Information Security Policy applies to all the entities forming part of the Nurture Group. For the purpose of this policy, 'entities' refers to group companies, affiliated companies, associates, and non-incorporated bodies that are considered part of the Nurture Group. These are referred to as "Group" throughout the rest of this policy.

This Policy applies to

- everyone working for the Group, meaning permanent, fixed term, or temporary staff; any third-party representatives, subcontractors, agency workers, volunteers, interns or agents engaged with the Group who have access to the Group's information systems, referred to as 'personnel', 'interested party' or 'user' in this document.
- all of Group's information systems which include all networks, hardware, end-point devices, databases, cloud-based systems, computer systems, equipment and software used by personnel working for the Group for storing, processing or transmitting the Group's information
- Nurture Group information, information of its employees and everyone working for Nurture Group, information of the Group's customers and third parties, processed, stored or transmitted by the Group. The words 'data' and 'information' are used interchangeably in this document as the context requires.

3 Roles and Responsibilities

The Board	Responsible for ensuring Nurture Group meets its legal obligations. It shall ensure that responsibilities for relevant roles are assigned and communicated within the Nurture Group. The Board shall appoint an independent expert as the Data Protection Officer for the Nurture Group.
Everyone who works for or on behalf of Nurture Group and who has access to the Nurture Group's information systems	Responsible for ensuring personal data is handled and processed in line with this Policy.
All members of staff	Have an obligation to report actual or potential data protection compliance failures as specified in our Acceptable Use Policy, so that Nurture Group's obligation of

	informing the Regulators and affected data subjects can be fulfilled within statutory time frames.

4 Identifying and recording uses of personal data

4.1 Data Review and Register

A Personal Data Register shall be established and maintained. The Personal Data Register shall detail data flow analysis that includes identification of:

- Key business processes that utilise personal data
- Sources of personal data
- Categories of personal data processed, including identification of high-risk and special category personal data
- The purpose for which each category of personal data is used, including subsequent secondary purposes over and above the initial purpose collected
- Potential recipients of personal data, key systems and repositories of personal data, offshore transfer, retention and disposal requirements.
- Whether Nurture Group is acting as data controller, processor or joint data controller

Regular data reviews to manage and mitigate risks shall be conducted regularly through updates to the information assets register. This includes information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

4.2 Data Protection Impact Assessment (DPIA)

The relevant head of the department shall carry out DPIA for all new projects and/or new uses of personal data which involve the use of new technologies, and the processing involved is likely to result in a high risk to the Privacy by Design and Default rights and freedoms of data subjects under the Data Protection Legislation.

DPIAs shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that shall be collected, held, and processed
- The purpose(s) for which personal data is to be used
- Nurture Group's objectives
- How personal data is to be used
- The parties (internal and/or external) who are to be consulted
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed
- Risks posed to data subjects
- Risks posed both within and to Nurture Group; and
- Proposed measures to minimise and handle identified risks
- DPIAs and evidence of consultation shall be retained and available for future reference.
- When designing or making significant changes to systems for use within Nurture Group or by its data processors, the Data Protection Officer shall ensure that compliance with privacy and data protection regulations is identified and managed from the start of such projects. The CIO shall be responsible for ensuring that all IT projects commence with a privacy plan.
- When relevant and when it does not have a negative impact on the data subject, privacy settings shall be set to the most private by default

4.3 Consent

- If the data that is collected is subject to consent by the data subject, such consent shall be obtained in a clear and transparent manner. This consent can be revoked at any time; it shall be ensured that the revocation of consent is easy for the data subjects.

- Any criminal record checks must be justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

5 Collection and Processing of Personal Data

5.1 Fair Lawful and transparent processing

- Personal data shall only be processed based on a legal basis (Appendix 0) which is recorded in the data register
- Information shall be provided to the data subjects in an appropriate format which clearly communicates
    - the purpose for which their personal data can be processed
    - the legitimate interest of Nurture Group
    - types of personal data collected
    - information about disclosure to third parties
    - transfer of such personal data outside the EU and safeguards in place
    - rights of the data subject
    - the retention period for their personal information
    - other information to make the processing fair and transparent
- The means by which an individual can object to processing by the Nurture Group shall be clearly explained in the following circumstances:
    - where the personal data is collected for marketing purposes or might be so used in future
    - where profiling by automated means is used for marketing purposes
- Any information presented to any individual shall be in a format easily accessible and understood by the intended audience.
- A record of privacy information (including privacy notices and online privacy statements) provided to individuals shall be maintained.

5.2 Processing for Specific Legitimate Purposes

- Any use of personal data shall be justified using at least one of the conditions for processing (Annexure 0), which shall be specifically documented. All staff responsible for processing personal data shall be aware of the conditions for processing.
- Personal data obtained for one purpose shall not be used for any unconnected purpose unless the individual concerned has explicitly agreed to this or a relevant exemption applies.

5.3 Adequate, Relevant and in line with data minimisation principles

- Any personal data collected shall be adequate for its purpose. Regular reviews of its technology and processes shall be conducted to ensure that the personal data continues to be adequate for its purposes.
- Nurture Group's systems and processes shall be reviewed annually to ensure the personal data being processed is relevant and not excessive.

5.4 Accuracy of Data and Keeping Data up to date

- Integrity and accuracy of personal data being processed shall be ensured.

- Any request by the individual to correct their personal data shall be promptly acted upon. If any personal data is found to be inaccurate or out of date, all reasonable steps shall be taken without delay to amend or erase that data, as appropriate.

5.5 Secure Processing

- All personal data collected, held, and processed shall be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- Detailed descriptions of all technical and organisational measures taken by it to ensure the security of personal data shall be maintained.
- Where Nurture Group shares personal data with a third party, the responsibilities of both parties with regard to personal data shall be formally documented in a written agreement or contract as appropriate.

5.6 Processing in accordance with the Individual's Rights

- Personal data shall be collected and processed lawfully, fairly, and transparently without adversely affecting the rights of the data subject.
- Any request from an individual to not use their personal data for direct marketing purposes shall be honoured and recorded in the relevant systems.
- Direct marketing material shall not be sent to someone electronically (e.g., via email) unless the Nurture Group has an existing business relationship with them in relation to the services being marketed or valid consent has been obtained from the subjects who are recipients of such marketing material.
- Please contact the Data Protection Officer for advice on direct marketing before starting any new direct marketing activity.
- A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

5.7 Subject Access Requests

- A data subject may make a subject access request (SAR) at any time to find out more about the personal data which Nurture Group holds about them. Subject access requests can be made in writing/email, by phone, in person, or on social media.
- Nurture Group shall respond to such request within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases, the data subject shall be informed of the need for the extension).
- All subject access requests received must be forwarded to Nurture Group's Data Protection Officer.
- No fee will be charged for the handling of normal SARs. However, reasonable fees may be charged for additional copies of information that has already been supplied to a data subject and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

6 Data Retention

- Personal data shall not be kept for any longer than is necessary for the purposes for which that data was originally collected and processed.
- The Personal Data Register shall identify the retention period for each type of personal data and shall
    - include any minimum retention period required by law and the retention period set by Nurture Group.
    - include justification and basis for the retention periods

- When the data is no longer required, all reasonable steps shall be taken to erase it without delay in accordance with the data destruction procedures (refer to Technical Security Standards).

7 Transferring Data Internationally

- Where personal data is transferred outside the UK by Nurture Group, it shall be ensured that the rights of the data subjects are protected.
- The Data Protection Officer shall review all new initiatives involving the transfer of personal data outside the EEA.
- The review shall establish that adequate protection can be provided to such transfers.
- The transfer of personal data to a country outside of the EEA shall take place only:
    - if the European Commission has assessed the country or territory as providing adequate protection
    - by including within contracts with specific and legally binding conditions which ensure the protection of personal information and the processing
    - by complying with an approved code of conduct or approved certification mechanism along with the binding and enforceable commitments on the destination organisation
    - for public bodies by complying with a legally binding and enforceable instrument or administrative arrangement

8 Security Issues

- Nurture Group's Information Security Policy shall specify security classification and measures as appropriate to the type of personal data being processed and the risk of damage or distress to the data subject if the information is compromised
- The Information Security Policy shall also ensure that
    - personal data is stored and handled securely, with precautions appropriate to its confidentiality and sensitivity
    - special attention is paid to the storage of personal data on removable media, portable devices and third-party storage systems (e.g., cloud storage)
    - electronic or manual transmission of personal data is secured by appropriate means
- The Data Protection Officer shall ensure that regular security assessments are undertaken to establish whether existing security controls around personal data are adequate and make recommendations for improvements if necessary.

9 Training

All staff shall receive training on data protection as appropriate to their job role. New joiners shall receive training as part of the induction process. Further training shall be provided at least every year or whenever there is a substantial change in the law or our policy and procedure.

Training can be provided through an in-house seminar, via online learning portals or any other means which are considered reasonable for this purpose on a regular basis. Completion of training shall be compulsory.

It shall cover the following:

- The law relating to data protection
- Nurture Group's data protection and related policies and procedures

10 Monitoring and Auditing

The DPO has responsibility for ensuring this policy is implemented and monitored appropriately.

11 Compliance

Adherence to this Policy is both an individual and a corporate responsibility. Wilful breach of this policy, or unauthorised departure from the Procedures derived from this Policy, may invoke the disciplinary procedure, which may also lead to the dismissal of an employee/contractor.

12 Review and Improvement

The DPO is responsible for reviewing this Policy, making any recommendations for improvement and presenting these to the ELT for further consideration.

Nurture Group reserves the right to amend or discontinue the Policy and any associated Procedures at any time.

Appendix: Legal Provisions

Personal Data

Any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject.

Data subject

A living, identified, or identifiable individual about whom Nurture Group holds personal data.

Data Protection Principles

The Data Protection Legislation sets out the following principles, which any party handling personal data must comply. All personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed,
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data shall be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to the implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Data Protection Legislation

All applicable data protection and privacy legislation, regulations and guidance, including, without limitation:

- the UK GDPR;
- the Data Protection Act 2018;
- and the Privacy and Electronic Communications Regulations (PECR); and
- any applicable guidance or codes of practice issued by the Information Commissioner from time to time

(All as amended, updated or re-enacted from time to time).

The Rights of Data Subjects

The Data Protection Legislation sets out the following key rights applicable to data subjects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object and
- Rights with respect to automated decision-making and profiling.

Legal Basis

The Data Protection Legislation seeks to ensure that personal data is processed lawfully, fairly, and transparently without adversely affecting the rights of the data subject. The Data Protection Legislation states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them
- The processing is necessary for compliance with a legal obligation to which the data controller is subject
- The processing is necessary to protect the vital interests of the data subject or of another natural person
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special Category Data

- If the personal data in question is "special category data" (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data), at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless prohibited by law)
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (if authorised by UK law)
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects
- The processing relates to personal data which is clearly made public by the data subject
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity
- The processing is necessary for substantial public interest reasons, with a basis in law, which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of UK and/or EU law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy) or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on the UK and/or EU law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Rules on International Transfers of Personal Data

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority
- The transfer is made with the informed consent of the relevant data subject(s)

- The transfer is necessary for the performance of a contract between the data subject and the Firm (or for pre-contractual steps taken at the request of the data subject)
- The transfer is necessary for important public interest reasons
- The transfer is necessary for the conduct of legal claims
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register