HEATHERLAND LTD
TRADING AS LUNNON PLANT & WASTE SERVICES

Data Protection Policy

Introduction

Heatherland Limited (The Company) takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously. This policy sets out how the company manages those responsibilities.

The Company obtains, uses, stores and otherwise processes personal data relating to current staff, former staff, clients, suppliers, contractors, and contacts, collectively referred to in this policy as data subjects. When processing personal data, the Company is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that we:

1. are clear about how personal data must be processed and the Company's expectations for all those who process personal data on its behalf;

2. comply with the data protection law and with good practice;

3. protect the Company's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights

4. protect the Company from risks of personal data breaches and other breaches of data protection law.

The main terms used are explained in the glossary at the end of this policy (Appendix 3).

Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the Company's behalf must read it. A failure to comply with this policy may result in disciplinary action.

The Managing Director is responsible for ensuring that all Company staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure that compliance.

The Company's Data Protection Officer (DPO) is Mr Michael Lunnon

Personal data protection principles

When you process personal data, you should be guided by the following principles, which are set out in the GDPR. The Company is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

1. processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency). Detail on how to achieve this can be found in Appendix 1.

2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation). Detail on how to achieve this can be found in Appendix 2.

3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation). Detail on how to achieve this can be found in Appendix 2.

4. accurate and where necessary kept up to date (Accuracy). Detail on how to achieve this can be found in Appendix 2.

5. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation). Detail on how to achieve this can be found in Appendix 2.

6. processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality). Detail on how to achieve this can be found in Appendix 2.

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. where the legal basis of our processing is Consent, to withdraw that Consent at any time;

2. to ask for access to the personal data that we hold (see below);

3. to prevent our use of the personal data for direct marketing purposes

4. to object to our processing of personal data in limited circumstances

5. to ask us to erase personal data without delay:

a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

b. if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;

c. if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;

d. if the data subject has objected to our processing for direct marketing purposes;

e. if the processing is unlawful.

6. to ask us to rectify inaccurate data or to complete incomplete data;

7. to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;

8. to ask us for a copy of the safeguards under which personal data is transferred outside of the EU;

9. the right not to be subject to decisions based solely on automated processing, including profiling,

except where necessary for entering into, or performing, a contract, with the Company; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;

10. to prevent processing that is likely to cause damage or distress to the data subject or anyone else;

11. to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

12. to make a complaint to the ICO; and

13. in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed

Requests (including for data subject access – see below) must be complied with, usually within one month of receipt. You must immediately forward any Data Subject Access Request you receive to the Information Compliance Team

Accountability

The Company must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Company is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

1. appointing a suitably qualified DPO;

2. implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects;

3. integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;

4. training staff on compliance with Data Protection Law and keeping a record accordingly; and

5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Responsibilities

1. Company responsibilities

As the Data Controller, the Company is responsible for establishing policies and procedures in order to comply with data protection law.

2. Data Protection Officer responsibilities

The DPO is responsible for:

(a) Advising the Company and its staff of its obligations under GDPR

(b) monitoring compliance with this Regulation and other relevant data protection law, the Company's policies with respect to this and monitoring training and audit activities relate to GDPR compliance

(c) to provide advice where requested on data protection impact assessments

(d) to cooperate with and act as the contact point for the Information Commissioner's Office

(e) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

3. Staff responsibilities

Staff members who process personal data about staff, clients or any other individual must comply with the requirements of this policy. Staff members must ensure that:

(a) all personal data is kept securely;

(b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;

(c) personal data is kept in accordance with the Company's retention schedule;

(d) any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Compliance team;

(e) any data protection breaches are swiftly brought to the attention of the Information Compliance team and the Data Protection Officer and that they support the Information Compliance team in resolving breaches;

(f) where there is uncertainty around a data protection matter advice is sought from the Information Compliance team and the Data Protection Officer.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Information Compliance team or the Data Protection Officer.

4. Third-Party Data Processors

Where external companies are used to process personal data on behalf of the Company, responsibility for the security and appropriate use of that data remains with the Company.

Where a third-party data processor is used:

(a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;

(b) reasonable steps must be taken that such security measures are in place;

(c) a written contract establishing what personal data will be processed and for what purpose must be set out;

(d) a data processing agreement, available from the Information Compliance team, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the Information Compliance team.

5. Contractors

The Company is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors must ensure that they are appropriately vetted for the data they will be processing. In addition managers should ensure that:

(a) any personal data collected or processed in the course of work undertaken for the Company is kept securely and confidentially;

(b) all personal data is returned to the Company on completion of the work, including any copies that may have been made. Alternatively that the data is securely destroyed and the Company receives notification in this regard from the contractor

(c) the Company receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;

(d) any personal data made available by the Company, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the Company;

(e) all practical and reasonable steps are taken to ensure that contractors do not have access to any personal data beyond what is essential for the work to be carried out properly.

Data subject Access Requests

Data subjects have the right to receive copy of their personal data which is held by the Company. In addition, an individual is entitled to receive further information about the Company's processing of their personal data as follows:

1. the purposes

2. the categories of personal data being processed

3. recipients/categories of recipient

4. retention periods

5. information about their rights

6. the right to complain to the ICO,

7. details of the relevant safeguards where personal data is transferred outside the EEA

8. any third-party source of the personal data

You should not allow third parties to persuade you into disclosing personal data without proper authorisation

The entitlement is not to documents per se (which may however be accessible by means of the Freedom of Information Act, subject to any exemptions and the public interest), but to such personal data as is contained in the document. The right relates to personal data held electronically and to limited manual records.

You should not alter, conceal, block or destroy personal data once a request for access has been made. You should contact the Information Compliance team before any changes are made to personal data which is the subject of an access request.

Reporting a personal data breach

The GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, you should immediately contact the Information Compliance team and follow the instructions in the personal data breach procedure. You must retain all evidence relating to personal data breaches in particular to enable the Company to maintain a record of such breaches, as required by the GDPR.

Limitations on the transfer of personal data

The GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit or send that data to a different country or view/access it in a different country.

You may only transfer personal data outside the EU if one of the following conditions applies:

1. the European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms. The countries currently approved can be found here:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

2. appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

3. the data subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or

4. the transfer is necessary for one of the other reasons set out in the GDPR including:

5. the performance of a contract between us and the data subject

6. reasons of public interest,

7. to establish, exercise or defend legal claims or

8. to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving Consent.

Record Keeping

The GDPR requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

These records should include, at a minimum, the name and contact details of the Company as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage

locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Records of personal data breaches must also be kept, setting out:

1. the facts surrounding the breach

2. its effects; and

3. the remedial action taken

Training and Audit

We are required to ensure that all Company staff undergo adequate training to enable them to comply with data protection law. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training.

You must regularly review all the systems and processes under your control to ensure they comply with this policy.

Data privacy by design and default and Data Protection Impact Assessments (DPIAs)

We are required to implement privacy-by-design measures when processing personal data, by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data-protection principles. The Company must ensure therefore that by default only personal data which is necessary for each specific purpose is processed. The obligation applies to the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons. You should ensure that you adhere to those measures.

As well as complying with Company wide practices designed to fulfil reasonable expectations of privacy, you should also ensure that your own data-handling practices default to privacy to minimise unwarranted intrusions in privacy e.g. by disseminating personal data to those who need to receive it to discharge their duties.

The Company must also conduct DPIAs in respect of high-risk processing before that processing is undertaken.

You should conduct a DPIA (and discuss your findings with the DPO) in the following circumstances:

1. the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

2. automated processing including profiling;

3. large scale processing of sensitive (special category) data; and

4. large scale, systematic monitoring of a publicly accessible area.

5. A DPIA must include:

6. a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;

7. an assessment of the necessity and proportionality of the processing in relation to its purpose;

8. an assessment of the risk to individuals; and

9. the risk-mitigation measures in place and demonstration of compliance.

Direct Marketing

We are subject to certain rules and privacy laws when marketing to our clients and any other potential user of our services.

For example, a data subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar services , and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a data subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Sharing Personal Data

In the absence of Consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to the Company

Some bodies have a statutory power to obtain information (e.g. regulatory bodies and government agencies such as the Child Support Agency). You should seek confirmation of any such power before disclosing personal data in response to a request. If you need guidance, please contact the Information Compliance team

Further, without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. You should seek written assurances from the police that the relevant exemption applies. If you need guidance, please contact the Information Compliance team

Some additional sharing of personal data for research purposes may also be permissible, subject to certain safeguards.

Changes to this policy

We reserve the right to change this policy at any time without notice to you so please check regularly to obtain the latest copy.

This policy was approved on 19th January 2022 by the Managing Director. It will be reviewed in January 2023.

Appendix 1

Principle 1 of GDPR – Processing personal data lawfully, fairly and transparently

1. **Lawfulness and fairness**

You may only process personal data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data for legitimate purposes without prejudicing the rights and freedoms of data subjects. In order to be justified, the University may only process personal data if the processing in question is based on one (or more) of the legal bases set out below. Section 4.3 below deals with justifying the processing of sensitive personal data. Including special category data.

The legal bases for processing non-sensitive personal data are as follows:

1. the data subject has given his or her Consent

2. the processing is necessary for the performance of a contract with the data subject

3. to meet our legal compliance obligations

4. to protect the data subject's vital interests (i.e. matters of life or death)

5. to pursue our legitimate interests (or another's legitimate interests) which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The specific legitimate interest or interests that the Company is pursuing when processing personal data will need to be set out in relevant Privacy Notices. This ground can only be relied upon for private functions e.g. marketing, fundraising and not for public functions.

You must identify the legal basis that is being relied on for each processing activity, which will be included in the Privacy Notice provided to data subjects.

(a) Consent

You should only obtain a data subject's Consent if there is no other legal basis for the processing. Consent requires genuine choice and genuine control.

A data subject consents to processing of his/her personal data if he/she indicates agreement clearly either by a statement or positive action to the processing. Silence, pre-ticked boxes or inactivity are therefore unlikely to be sufficient. If Consent is given in a document that deals with other matters, you must ensure that the Consent is separate and distinct from those other matters.

Data subjects must be able to withdraw Consent to processing easily at any time. Withdrawal of Consent must be promptly honoured. Consent may need to be renewed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented, or if the Consent is historic.

You will need to ensure that you have evidence of Consent and you should keep a record of all Consents obtained so that we can demonstrate compliance.

Consent is required for some electronic marketing and some research purposes.

(b) Legal bases for Processing Sensitive Personal Data, including Special Category Data

Special Category Personal Data is data revealing:

1. racial or ethnic origin

2. political opinions

3. religious or philosophical beliefs,

4. trade union membership,

It also includes the processing of:

5. genetic data

6. biometric data for the purpose of uniquely identifying a natural person,

7. data concerning health

8. data concerning a natural person's sex life or sexual orientation

Personal data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences should be treated in the same way to special category data.

The processing of sensitive personal data by the Company must be based on one of the following (together with one of the legal bases for processing non-sensitive personal data as listed above):

1. the data subject has given explicit Consent (requiring a clear statement, not merely an action)

2. the processing is necessary for complying with employment law;

3. the processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving Consent;

4. the processing relates to personal data which are manifestly made public by the data subject;

5. the processing is necessary for the establishment, exercise or defence of legal claims;

6. the processing is necessary for reasons of substantial public interest (provided it is proportionate to the particular aim pursued and takes into account the privacy rights of the data subject)

7. the processing is necessary for the purposes of preventive or occupational medicine, etc. provided that it is subject to professional confidentiality

8. the processing is necessary for reasons of public interest in the area of public health, provided it is subject to professional confidentiality;

9. the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if it is subject to certain safeguards (i.e. pseudonymisation

or anonymisation where possible, the research is not carried out for the purposes of making decisions about particular individuals (unless it is approved medical research) and it must not be likely to cause substantial damage/distress to an individual and is in the public interest).

Examples of sensitive personal data processed by the Company will include:

1. details of relevant unspent convictions for the purposes of assessing eligibility

2. details of relevant unspent convictions for the purposes of recruiting relevant staff

3. checks conducted by the Disclosure and Barring Service for the purposes of assessing eligibility of staff to engage in work with children and vulnerable adults, as permitted by legislation relating to the rehabilitation of offenders or for determining fitness to practise relevant professions

4. unspent convictions or allegations of sexual misconduct for staff and student disciplinary purposes

5. health data for the purposes for assessing eligibility to undertake relevant professional programmes, assessing fitness to study or to engage in Company activities

6. details of disability for the purposes of assessing and implementing reasonable adjustments to the Company's policies, criteria or practices

7. details of racial/ethnic origin, sexual orientation, religion/belief for the purposes of equality monitoring

Processing sensitive personal data represents a greater intrusion into individual privacy than when processing non-sensitive personal data. You must therefore take special care when processing sensitive personal data and ensure that you comply with the data protection principles (as set out in the main body of this policy) and with this policy, in particular in ensuring the security of the sensitive personal data.

2. Transparency (notifying data subjects)

Under the GDPR the Company is required to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. That information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand what happens to their personal data.

Whenever we collect personal data directly from data subjects, for example for the recruitment and employment of staff, at the time of collection we must provide the data subject with all the prescribed information which includes:

1. Company's details

2. Contact details of DPO

3. Purposes of processing

4. Legal basis of processing

5. Where the legal basis is legitimate interest, identify the particular interests (e.g. marketing, fundraising)

6. Where the legal basis is Consent, the right to withdraw

7. Where statutory/contractual necessity, the consequences for the Data Subject of not providing the data of non-provision

When personal data is collected indirectly (for example, from a third party or publically available source), you must also provide information about the categories of personal data and any information on the source. The data subject must be provided with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

Appendix 2

Principle 2 of GDPR - Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot therefore use personal data for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless you have informed the data subject of the new purposes. Where the further processing is not based on the data subject's Consent or on a lawful exemption from data-protection law requirements, you should assess whether a purpose is incompatible by taking into account factors such as:

1. the link between the original purpose/s for which the personal data was collected and the intended further processing

2. the context in which the personal data has been collected – in particular the Company-data subject relationship. You should ask yourself if the data subject would reasonably anticipate the further processing of his/her personal data

3. the nature of the personal data in particular whether it involves special categories of personal data (i.e. sensitive) or personal data relating to criminal offences/convictions

4. the consequences of the intended further processing for the data subjects

5. the existence of any appropriate safeguards e.g. encryption or pseudonymisation.

Provided that prescribed safeguards are implemented, further processing for scientific or historical research purposes or for statistical purposes will not be regarded as incompatible. Safeguards include ensuring data minimisation (e.g. pseudonymisation or anonymisation where possible), the research will not be carried out for the purposes of making decisions about particular individuals and

it must not be likely to cause substantial damage/distress to an individual, unless it is approved medical research.

Principle 3 of the GDPR – Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You should not therefore amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. Conversely, personal data must be adequate to ensure that we can fulfil the purposes for which it was intended to be processed.

You may only process personal data when performing your job duties requires it and you should not process personal data for any reason unrelated to your job duties.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the University's data retention policy and schedule.

Principle 4 of the GDPR - Accuracy

Personal data must be accurate and, where necessary, kept up to date. You should ensure that personal data is recorded in the correct files.

Incomplete records can lead to inaccurate conclusions being drawn and in particular, where there is such a risk, you should ensure that relevant records are completed.

You must check the accuracy of any personal data at the point of collection and at regular intervals thereafter. You must take all reasonable steps to destroy or amend inaccurate records without delay and you should up-date out-of-date personal data where necessary (e.g. where it is not simply a pure historical record).

Where a data subject has required his/her personal data to be rectified or erased, you should inform recipients of that personal data that it has been erased/rectified, unless it is impossible or significantly onerous to do so.

Principle 5 of the GDPR – Storage limitation

You must not keep personal data in a form that allows data subjects to be identified for longer than needed for the legitimate Company business purposes or other purposes for which the Company collected it. Those purposes include satisfying any legal, accounting or reporting requirements. Records of personal data can be kept for longer than necessary if anonymised.

You will take all reasonable steps to destroy or erase from the Company's systems all personal data that we no longer require in accordance with all relevant Company records retention schedules and policies. The Company has a document retention policy.

You will ensure that data subjects are informed of the period for which their personal data is stored or how that period is determined in any relevant Privacy Notice.

Principle 6 of the GDPR – Security, Integrity and Confidentiality

The Company is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorised or unlawful processing or accidental loss, destruction of, or damage to their personal data. Safeguarding will include the use of encryption and pseudonymisation where appropriate. It also

includes protecting the confidentiality (i.e. that only those who need to know and are authorised to use personal data have access to it), integrity and availability of the personal data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

You are also responsible for protecting the personal data that you process in the course of your duties. You must therefore handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

You must comply with all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.

You must comply with all applicable aspects of our Information Security Policy, and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Law standards to protect personal data.

You may only transfer personal data to third-party service providers (i.e. data processors) who provide sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Law and who agree to act only on the Company's instructions. Data processors should therefore be appointed subject to the Company's standard contractual requirements for data processors.

Appendix 3

Glossary of Terms

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not automated processing.

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data Controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with the GDPR. The Company is the Data Controller of all personal data relating to it and used for all other purposes connected with it including business purposes. .

Data Subject: a living, identified or identifiable individual about whom we hold personal data.

Data Protection impact assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be

conducted for all major system or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person appointed as such under the GDPR and in accordance with its requirements. A DPO is responsible for advising the Company (including its employees) on their obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with the Company's polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

Personal Data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

Privacy by Design and Default: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to data subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Michael D Lunnon

05th January 2023