V1CE Limited

GDPR Privacy and Personal Data Protection Policy VCEGDPR001

Document Ref:	GDPR Privacy and Personal Data Protection Policy
Version:	5.0
Date of Version:	20/11/2025
Created By:	Roger Hadley
Updated By:	Akshay Kumar
Approved By:	Francis Falodun
Confidentiality Level:	Controlled: Uncontrolled if printed

Amendment History

Date	Version	Created By	Description of Change
10 May 2020	1.0	Company Directors	Initial Release
01 Aug 2022	2.0	Operations Manager	Review – Transition of Providers
03 Nov 2022	3.0	Operations Manager	Update Of Variations
04 Mar 2024	4.0	Operations Manager	Update Of Variations
20 Nov 2025	5.0	Operations Manager	Update Of Variations

Table of Contents

1 Introduction

In its everyday business operations, V1CE Limited makes use of a variety of data about identifiable individuals, including data about:

- Current, past, and prospective employees
- Customers
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps V1CE Limited is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, directors, employees, suppliers and other third parties who have access to V1CE Limited systems.

The following policies and procedures are relevant to this document:

- Privacy Policy
- Customer Data Procedure
- Data Request Procedure
- Data Breach Procedure
- Staff Employment Documentation
- Data Protection Impact Assessment
- Personal Data Storage Reviews
- Employee Data Review
- Records Retention and Protection Policy

2. Privacy and Personal Data Protection Policy

This can be found at www.v1ce.co

2.1. The General Data Protection Regulation

The General Data Protection Regulation 2018 (GDPR) is one of the most significant pieces of legislation affecting the way that V1CE Limited carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is V1CE Limited's policy to ensure that our compliance with the GDPR and other relevant legislation is always clear and demonstrable.

2.2. Definitions

There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 natural person.

'processing' means:

any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'controller' means:

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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

2.3. Principles Relating to Processing of Personal Data

There are several fundamental principles upon which the GDPR is based.

These are as follows:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

(b) 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, in accordance with Article 89(1), not be incompatible with the initial purposes ('purpose limitation').

(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods

insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

V1CE Limited will ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

2.4. Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within V1CE Limited that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown in the Data Request Procedure at annex a

2.5. Lawfulness of Processing

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is V1CE Limited policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief in the following sections.

2.6. Consent

Unless it is necessary for a reason allowable in the GDPR, V1CE Limited will always obtain explicit consent from a data subject to collect and process their data. In case of children below the age of 16 (a lower age may be allowable in specific EU member states) parental consent will be obtained. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject, then this information will be provided to the data subject within a reasonable period after the data are obtained and within one month.

2.7. Performance of a Contract

Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. a delivery cannot be made without an address to deliver to.

2.8. Legal Obligation

If the personal data is required to be collected and processed to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.

2.8.1. Vital Interests of the Data Subject

In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. V1CE will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used in aspects of social care, particularly in the public sector.

2.8.2. Task Carried Out in the Public Interest

Where V1CE Limited needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

2.8.3. Legitimate Interests

If the processing of specific personal data is in the legitimate interests of V1CE Limited and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

2.9. Privacy by Design

V1CE Limited has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

• Consideration of how personal data will be processed and for what purposes • Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
• Assessment of the risks to individuals in processing the personal data
• What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate. See V1CE Limited Privacy Policy at annex A

2.10. Contracts Involving the Processing of Personal Data

V1CE Limited will ensure that all relationships it enters that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR. Staff to advise new customers to refer to the Privacy Policy.

See Data Breach Procedure at Annex B
See Customer Data Procedure at Annex C
See Staff Employment Data Procedure at Annex D
GDPR Data Request Procedure available on request at support@v1ce.co
See GDPR Audit Procedure at Annex F
See Communication Policy at Annex G
See Subject Access Policy at Annex H
See Variation of Terms & Conditions at Annex J
See Data Protection Policy at Annex K

2.11. International Transfers of Personal Data

Transfers of personal data outside the European Union will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

V1CE Limited does not transfer data outside the UK / EU at present

2.12. Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in house resource or outsourced to an appropriate service provider.

Based on these criteria, V1CE Limited has appointed a data protection officer.

2.13. Breach Notification

It is V1CE Limited policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our Data Breach Procedure which sets out the overall process of handling information security incidents. See annex B

Under the GDPR the relevant DPA has the authority to impose a range of fines of up to four percent of annual turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

2.14. Addressing Compliance to the GDPR

The following actions are undertaken to ensure that V1CE Limited always complies with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organisation (if required)
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Procedures are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes •

The following documentation of processing activities is recorded:

- Organisation name and relevant details
- Purposes of the personal data processing
- Categories of individuals and personal data processed
- Categories of personal data recipients
- Personal data retention schedules
- Relevant technical and organisational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with data protection.

See Audit Review Procedure at annex F

3. Associated Documented Information

Document Reference	Storage Location	Document Owner	Controls For Record Protection	Retention Period
GDPR Policies / Procedures	HSE Secure Server / Hard Copies in File	Financial Director	Controlled: Restricted Access	7 Years / Continuous
GDPR Training Guides	HSE Secure Server / Hard Copies in File	Financial Director	Controlled: Restricted Access	7 Years / Continuous
GDPR DPIA / Reviews	HSE Secure Server / Hard Copies in File	Financial Director	Controlled: Restricted Access	7 Years / Continuous
GDPR Implementation Plan	HSE Secure Server / Hard Copies in File	Financial Director	Controlled: Restricted Access	7 Years
GDPR ICO Registration	HSE Secure Server / Hard Copies in File	Financial Director	Controlled: Restricted Access	7 Years / Continuous
GDPR Data Cleanse Records	HSE Secure Server / Hard Copies in File	Financial Director	Controlled: Restricted Access	7 Years
GDPR Breaches	HSE Secure Server / Hard Copies in File	Financial Director	Controlled: Restricted Access	7 Years
GDPR Requests	HSE Secure Server / Hard Copies in	Financial Director	Controlled: Restricted Access	7 Years

	File			

We are committed to protecting and respecting your privacy.
This Policy explains when and why we collect personal information about people who contact us, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

1. Who we are?

V1CE Limited are committed to protecting and respecting your privacy. We are the data controller. This means we decide how your personal data is processed and for what purposes.
We are also the processor for any 3rd parties for the benefit of providing services to our customers e.g., lead capture.

2. Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in, or likely to come into, the data controller's possession. The processing of personal data is governed by the General Data Protection Regulation (GDPR).

Data collected:
• Name
• Address
• Contact Details – E-mail, address and telephone numbers, Voice, and video recordings of Zoom meetings. (Some of which we may obtain from an online or public business directory when necessary) Images on CCTV.

3. How do we process your personal data?

We comply with our obligations under the Data Protection Act (DPA) and the General Data Protection Regulation (GDPR) by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access, and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

4. What is the legal basis for processing your personal data?

The uses of your data detailed along with the basis for each one.

Contract	To process, and keep you informed of the progress of, an order	Processing is necessary for us to fulfil either a verbal or written contract for the supply of goods or services.
Consent	To carefully selected partners	We will only use your data for this purpose when necessary for compliance.
Legal Obligation	Data on invoices	Processing is necessary for compliance with a legal / statutory obligation.
Legitimate Interest	To advise you of updates and features that have been developed through our application.	Processing is necessary for us to carry out our duty of care and to ensure all customers

	To update the manufacturer with your current contact details and delivery service information	receive a level of service in line with your, our expectations.
	To maintain our own accounts and records.	
	To employ staff.	Processing is necessary for various government bodies.

5. What Are Your Rights?

Under the GDPR, you have the following rights, which we will always work to uphold: The right to be informed about our collection and use of your personal data. This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions.
The right to access the personal data we hold about you.
The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete.
The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we have.
The right to restrict (i.e. prevent) the processing of your personal data. The right to object to us processing your personal data for a particular purpose or purposes. The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data. Rights relating to automated decision-making and profiling. (We do not use your personal data in this way.)
For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 11 to find out more – in some cases the legal obligation may over-ride your rights.
Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau. If you have any cause for complaint about our use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.

6. How Do We Use Personal Data?

Under the GDPR, we must always have a lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, because you have consented to our use of your personal data, or because it is in our legitimate business interests to use it. Your personal data may be used for one of the following purposes:
•Providing and managing your account

•Supplying our products AND/OR services to you. Your personal details are required in order for us to enter into a contract with you.
•Communicating with you. This may include responding to emails or calls from you. We will always work to fully protect your rights and comply with our obligations under the GDPR Regulations.

7. How Long Will We Keep My Personal Data?

We will not keep your personal data for any longer than is necessary considering the reason(s) for which it was first collected. Your personal data will therefore be kept for the following periods (or, where there is no fixed period, the following factors will be used to determine how long it is kept):

Your personal data will be retained for a period of 10 years from the date of you last contact with us.

8. How and Where Do We Store or Transfer Your Personal Data?

Personal data is stored and transferred through several sub processors these sub processors are necessary to allow us to fulfil and complete delivery of our product and services.

Entity	**Service Provided**	**Data Location**
myLoc	App Web Hosting	EU
Zendesk	CRM system	EU
Make.com	Automation Processor	EU
Zoom	Audio and Video call recordings	EU
Shopify	E-commerce Platform	EU
Klaviyo	Marketing Platform	EU
Calendly	Calendar Service Provider	EU
Stripe	Payment Processing Provider	EU
Ship theory	Delivery Partner	

9. Do We Share Your Personal Data?

We will not share any of your personal data with any third parties unless it is necessary or of benefit to you and the service we provide.

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

10. How Can You Access Your Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a "subject access request".

All subject access requests should be made in writing and sent to the email or postal address shown in Paragraph 11.

There is not normally any charge for a subject access request. If your request is 'manifestly unfounded or excessive' (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your subject access request within 28 Days and, in any case. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

11. How Do You Contact Us?

To contact us about anything to do with your personal data and data protection, including to make a subject access request, please use the following details -
Email address: support@v1ce.co
Telephone number: TBC

12. Changes to this Privacy Notice

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection. Any changes will be made available via our website.

13. Further Guidance / Enquiries / Complaints

https://www.gov.uk/data-protection
https://ico.org.uk/

V1CE GDPR Annex

DATA BREACH NOTIFICATION POLICY

A) AIM

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

B) PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or processed.

The following are examples of data breaches:

a) access by an unauthorised third party.
b) deliberate or accidental action (or inaction) by a data controller or data processor.
c) sending personal data to an incorrect recipient.
d) computing devices containing personal data being lost or stolen.
e) alteration of personal data without permission.
f) loss of availability of personal data.

C) BREACH DETECTION MEASURES

We have implemented the following measures to assist us in detecting a personal data breach: Data Protection Officer and Audits

D) INVESTIGATION INTO SUSPECTED BREACH

If we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by Roger Hadley, Operations Manager who will decide over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

E) WHEN A BREACH WILL BE NOTIFIED TO THE INFORMATION COMMISSIONER

In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms

can include physical, material, or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

a) a description of the nature of the personal data breach including, where possible:

i) the categories and approximate number of individuals concerned; and
ii) the categories and approximate number of personal data records concerned

b) the name and contact details of the data protection officer where more information can be obtained.
c) a description of the likely consequences of the personal data breach; and d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

F) WHEN A BREACH WILL BE NOTIFIED TO THE INDIVIDUAL

In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

a) a description of the nature of the breach
b) the name and contact details of the data protection officer where more information can be obtained
c) a description of the likely consequences of the personal data breach and d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

G) RECORD OF BREACHES

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

POLICY ON YOUR RIGHTS IN RELATION TO YOUR DATA

A) AIM

This policy outlines the rights that data subjects have, under the General Data Protection Regulation (GDPR), in relation to the data about them that we hold. Data subjects, for the purposes of this policy, includes employees (current, prospective, and former), workers and contractors.

B) THE RIGHT TO BE INFORMED

In order to keep you informed about how we use your data, we have a privacy notice for employees. You can obtain a copy of the privacy notice from your manager.

The Company also has a separate privacy notice applicable to job applicants, available from your manager.

You will not be charged for receiving our privacy notices.

Our privacy notices set out:

a) the types of data we hold and the reason for processing the data.
b) our legitimate interest for processing it.
c) details of who your data is disclosed to and why, including transfers to other countries. Where data is transferred to other counties, the safeguards used to keep your data secure are explained.
d) how long we keep your data for, or how we determine how long to keep your data for.
e) where your data comes from.
f) your rights as a data subject.
g) your absolute right to withdraw consent for processing data where consent has been provided and no other lawful reason for processing your data applies.
h) your right to make a complaint to the Information Commissioner if you think your rights have been breached.
i) whether we use automated decision making and if so, how the decisions are made, what this means for you and what could happen as a result of the process.
j) the name and contact details of our data protection officer.

C) THE RIGHT OF ACCESS

You have the right to access your personal data which is held by us. You can find out more about how to request access to your data by reading our Subject Access Request policy.

D) THE RIGHT TO 'CORRECTION'

If you discover that the data, we hold about you is incorrect or incomplete, you have the right to have the data corrected. If you wish to have your data corrected, you should complete the Data Correction Form.

Usually, we will comply with a request to rectify data within one month unless the request is particularly complex in which case we may write to you to inform you we require an extension to the normal timescale. The maximum extension period is two months.

You will be informed if we decide not to take any action because of the request. In these circumstances, you can complain to the Information Commissioner and have access to a judicial remedy.

Third parties to whom the data was disclosed will be informed of the rectification.

E) THE RIGHT OF 'ERASURE'

In certain circumstances, we are required to delete the data we hold about you. Those circumstances are:

a) where it is no longer necessary for us to keep the data.
b) where we relied on your consent to process the data and you subsequently withdraw that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data.
c) where you object to the processing (see below) and the Company has no overriding legitimate interest to continue the processing.
d) where we have unlawfully processed your data.
e) where we are required by law to erase the data.

If you wish to make a request for data deletion, you should complete the Data Erasure form.

We will consider each request individually, however, you must be aware that processing may continue under one of the permissible reasons. Where this happens, you will be informed of the continued use of your data and the reason for this.

Third parties to whom the data was disclosed will be informed of the erasure where possible unless to do so will cause a disproportionate effect on us.

F) THE RIGHT OF 'RESTRICTION'

You have the right to restrict the processing of your data in certain circumstances. We will be

required to restrict the processing of your personal data in the following circumstances:

a) where you tell us that the data, we hold on to you is not accurate. Where this is the case, we will stop processing the data until we have taken steps to ensure that the data is accurate.
b) where the data is processed for the performance of a public interest task or because of our legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether our legitimate interests mean it is appropriate to continue to process it.
c) when the data has been processed unlawfully.
d) where we no longer need to process the data, but you need the data in relation to a legal claim.

If you wish to make a request for data restriction, you should complete the Data Restriction form.

Where data processing is restricted, we will continue to hold the data but will not process it unless you consent to the processing or processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible unless to do so will cause a disproportionate effect on us.

You will be informed before any restriction is lifted.

G) THE RIGHT TO DATA 'PORTABILITY'

You have the right to obtain the data that we process on you and transfer it to another party. Where our technology permits, we will transfer the data directly to the other party.

Data which may be transferred is data which:

a) you have provided to us; and
b) is processed because you have provided your consent or because it is needed to perform the employment contract between us; and
c) is processed by automated means.

If you wish to exercise this right, please speak to your manager.

We will respond to a portability request without undue delay, and within one month at the latest unless the request is complex, or we receive a number of requests in which case we may write to you to inform you that we require an extension and reasons for this. The maximum extension period is two months.

We will not charge you for access to your data for this purpose.

You will be informed if we decide not to take any action because of the request, for example, because the data you wish to transfer does not meet the above criteria. In these circumstances, you can complain to the Information Commissioner and have access to a judicial remedy.

The right to data portability relates only to data defined as above. You should be aware that this differs from the data which is accessible via a Subject Access Request.

H) THE RIGHT TO 'OBJECT'

You have a right to require us to stop processing your data; this is known as data objection.

You may object to processing where it is carried out:

a) in relation to the Company's legitimate interests.
b) for the performance of a task in the public interest.
c) in the exercise of official authority; or
d) for profiling purposes.

If you wish to object, you should do so by completing the Data Objection Form. In some

circumstances we will continue to process the data you have objected to. This may occur when:

a) we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights; or
b) the processing is required in relation to legal claims made by, or against, us. If the

response to your request is that we will take no action, you will be informed of the reasons.

I) RIGHT NOT TO HAVE AUTOMATED DECISIONS MADE ABOUT YOU

You have the right not to have decisions made about you solely based on automated decision-making processes where there is no human intervention, where such decisions will have a significant effect on you.

However, the Company does not make any decisions based on such processes.

In circumstances where we use special category data, for example, data about your health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership the Company will ensure that one of the following applies to the processing:

a) you have given your explicit consent to the processing; or

b) the processing is necessary for reasons of substantial public interest.

PRIVACY NOTICE FOR EMPLOYEES

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you, our employees, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This notice applies to current and former employees and workers.

A) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing is fair, lawful, and transparent
b) data is collected for specific, explicit, and legitimate purposes
c) data collected is adequate, relevant, and limited to what is necessary for the purposes of processing
d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage by using appropriate technical or organisation measures
g) we comply with the relevant GDPR procedures for international transferring of personal data

B) TYPES OF DATA HELD

We keep several categories of personal data on our employees to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems.

Specifically, we hold the following types of data, as appropriate to your status:

a) personal details such as name, address, phone numbers
b) name and contact details of your next of kin
c) your photograph
d) your gender, marital status, information of any disability you have or other medical information
e) right to work documentation
f) information on your race and religion for equality monitoring purposes
g) information gathered via the recruitment process such as that entered a CV or included in a CV cover letter
h) references from former employers
i) details on your education and employment history etc
j) National Insurance numbers
k) bank account details
l) tax codes
m) driving licence
n) criminal convictions

o) information relating to your employment with us, including:

i) job title and job descriptions
ii) your salary
iii) your wider terms and conditions of employment
iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal, and performance information
v) internal and external training modules undertaken
vi) information on time off from work including sickness absence, family related leave etc

p) IT equipment use including and internet access.

C) COLLECTING YOUR DATA

You provide several pieces of data to us directly during the recruitment period and subsequently upon the start of your employment.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in files or within the Company's HR and IT systems.

D) LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data to comply with a legal requirement or to effectively manage the employment contract we have with you, including ensuring you are paid correctly.

The information below categorises the types of data processing, appropriate to your status, we undertake and the lawful basis we rely on.

Activity requiring your data	**Lawful basis**
Carry out the employment contract that we have entered with you e.g., using your name, contact details, education history, information on any disciplinary, grievance procedures involving you	Performance of the contract
Ensuring you are paid	Performance of the contract
Ensuring tax and National Insurance is paid	Legal obligation
Carrying out checks in relation to your right to work in the UK	Legal obligation
Making reasonable adjustments for disabled employees	Legal obligation
Making recruitment decisions in relation to both initial and subsequent employment e.g., promotion	Our legitimate interests

Making decisions about salary and other benefits	Our legitimate interests
Ensuring efficient administration of contractual benefits to you	Our legitimate interests
Effectively monitoring both your conduct, including timekeeping and attendance, and your performance and to undertake procedures where necessary	Our legitimate interests

Maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained	Our legitimate interests
Implementing grievance procedures	Our legitimate interests
Assessing training needs	Our legitimate interests
Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments	Our legitimate interests
Gaining expert medical opinion when making decisions about your fitness for work	Our legitimate interests
Managing statutory leave and pay systems such as maternity leave and pay etc	Our legitimate interests
Business planning and restructuring exercises	Our legitimate interests
Dealing with legal claims made against us	Our legitimate interests
Preventing fraud	Our legitimate interests
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests
Providing employment references to prospective employers, when our name has been put forward by the employee/ex-employee, to assist with their effective recruitment decisions	Legitimate interest of the prospective employer

E) SPECIAL CATEGORIES OF DATA

Special categories of data are data relating to your:

a) health
b) sex life

c) sexual orientation
d) race
e) ethnic origin
f) political opinion
g) religion
h) trade union membership
i) genetic and biometric data.

We carry out processing activities using special category data:

a) for the purposes of equal opportunities monitoring
b) in our sickness absence management procedures
c) to determine reasonable adjustments

Most commonly, we will process special categories of data when the following applies:

a) you have given explicit consent to the processing
b) we must process the data to carry out our legal obligations
c) we must process data for reasons of substantial public interest
d) you have already made the data public.

F) FAILURE TO PROVIDE DATA

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering a contract of employment with you. This could include being unable to offer you employment or administer contractual benefits.

G) CRIMINAL CONVICTION DATA

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data to determine your suitability, or your continued suitability for the role. We rely on the lawful basis set out in Article 6 of the UK GDPR to process this data.

H) WHO WE SHARE YOUR DATA WITH

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processing in line with GDPR.

Data is shared with third parties for the following reasons: administration of payroll, employee expenses and administration of our pension scheme.

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us. We have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

I) PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction, and abuse. We have implemented processes to guard against such.

J) RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Some data retention periods are set by the law. Our retention periods are Retention periods can vary depending on why we need your data, as set out below:

- Payroll records – No more than 6 years after the end of the financial year to which they relate – Taxes Management Act 1970.
- Records relating to working time – No more than 2 years from the date to which they were made – Working Time Regulations 1998.
- Accident Records: Minimum of 3 years since the last entry, or if it involves a child until they reach 21.
- Income Tax and NI: Minimum of 3 years from the end of the financial year to which they relate. •

Maternity and Paternity: Minimum of 3 years from the end of the tax year in which the leave ends.

- Application and Recruitment Records: No more than 12 months after the date of termination of

the employee. https://pages.peninsulagrouplimited.com/EOD-Harassment-Building-a-safe

workplace.html

- Parental Leave: 5 years from birth or adoption, or 18 years if the child receives a disability allowance.
- Pension Benefits: 12 years from the ending of any benefit payable.
- All Personnel Files, Training Records and Sickness Absence Records: 6 years from the end of employment.
- Redundancy Records: 6 years from the end of employment.

K) AUTOMATED DECISION MAKING

Automated decision-making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely based on automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

L) EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it; b) the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests.
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data.
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information.

h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

M) CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

N) MAKING A COMPLAINT

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

O) DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:
_____(Name)
_____(Contact details).

V1CE Data Protection Audit Form

Category of personal data:	
What is the purpose for processing the data?	
What category of person does the data relate to?	
What is the source of the data?	
What date was the data collected?	
Where is the data stored?	
Is it live data or archived?	

How long is the data retained for?	
Was a privacy notice issued?	
Does a privacy notice need to be re-issued?	
Has the employee been made aware of their rights in relation to this data ie erasure, rectification, restriction, objection?	
Does the data fall into the "special categories" definition?	
Does the data relate to criminal convictions?	
Does the data involve automated decision	

making? If so, what decisions are made and what are the consequences will the decisions have on individuals?	
Who is responsible for ensuring accuracy of data?	
Who has access to the data?	

Are security controls in place to restrict access to this data? What are they?	
Is the data shared with anyone outside of the organisation? If so, who?	
Is the data shared with anyone outside of the EEA? If so, which countries is the data transferred to?	
How is the data destroyed when it is at the end of the retention period?	
What current policies apply to the data in question?	
Are these policies up to date?	

Which of the lawful bases for processing the data applies?	
If data is 'special' category, which of the lawful bases for processing the data applies?	

Annex G

COMMUNICATIONS POLICY

A) INTRODUCTION

1) IT and Communication plays an essential role in the conduct of our business. The IT infrastructure including e mail and internet access have therefore significantly improved business operations and efficiencies.

2) How you communicate with people not only reflects on you as an individual but also on us as a business. As a result of this the company values your ability to communicate with colleagues, clients/customers, and business contacts but we must also ensure that such systems and access are managed correctly, not abused in how they are used or what they are used for.

3) This policy applies to all members of the Company who use our or our clients' communications facilities, whether Directors/Consultants, full or part-time employees, contract staff or temporary staff. The parameters and restrictions are outlined below and you are required to read them carefully.

B) GENERAL PRINCIPLES

1) You must use our and our clients' information technology and communications facilities sensibly, professionally, lawfully, consistently with your duties and in accordance with this policy and other Company rules and procedures.

2) At all times employees must behave with honesty and integrity and respect the rights and privacy of others in relation to electronic communication and information. The company reserves the right to maintain all electronic communication and files.

3) Every employee will be given access to the Intranet and/or Internet as appropriate to their job needs. For those who do not have daily PC access occasional access will be arranged, as necessary, by Management,

4) All PC/network access will be through passwords, and no individual is permitted onto the system using another employee's password. Employees are not permitted to share their password with anyone inside or outside the company. Individuals will be allowed to set their own passwords and must change them as frequently as requested by the system set-up requirements.

5) All information relating to our clients/customers and our business operations is confidential. You must treat our paper-based and electronic information with utmost care.

6) Many aspects of communication are protected by intellectual property rights which can be infringed in several ways. Downloading, copying, possessing, and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

7) Care must be taken when using e-mail as a means of communication because all expressions of fact, intention and opinion in an e-mail may bind you and/or the Company and can be produced in court in the same way as other kinds of written statements.

8) If you are speaking with someone face to face, via the telephone, in writing via whatever medium you are a representative of the Company. Whilst in this role you should not express any personal opinion that you know, or suspect might be contrary to the opinions of the Directors or Company policy.

9) You must not use any of our or our clients' media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any sexist, racist, defamatory, or other unlawful material. If you are in doubt about a course of action, take advice from a member of management.

C) USE OF ELECTRONIC MAIL

1) **Business use**

Always use the "Bcc" box when mailing to groups whenever the members of the group are unaware of the

identity of all the others (as in the case of marketing mailing lists), or where you judge that the membership of the group of one or more individuals should perhaps not be disclosed to the others (as in the case of members of a staff benefit scheme), because if you use the "Cc" box each recipient is informed of the identity (and in the case of external recipients, the address) of all the others. Such a disclosure may breach any duty of confidence owed to each recipient, breach the Company's obligations under the General Data Protection Regulation and Data Protection Act or may inadvertently disclose confidential business information such as a marketing list. This applies to both external and internal e-mail. Expressly agree with the customer/client that the use of e-mail is an acceptable form of communication bearing in mind that if the material is confidential, privileged or commercially sensitive then un-encrypted e-mail is not secure.

If you have sent an important document, always telephone to confirm that the e-mail has been received and read.

Considering the security risks inherent in web-based e-mail accounts, you must not e-mail business documents to your personal web-based accounts. You may send documents to a customer's/client's web-based account if you have the customer's/client's express written permission to do so. However, under no circumstances should you send sensitive or highly confidential documents to a customer's/client's personal web-based e-mail account (e.g. Yahoo, or Hotmail), even if the customer/client asks you to do so.

2) **Personal use**

a) Although our e-mail facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, the Company may need to monitor communications for the reasons shown below.

b) Under no circumstances may the Company's facilities be used in connection with the operation or management of any business other than that of the Company or a customer/client of the Company unless express permission has been obtained from a member of management.

c) You must ensure that your personal e-mail use:

• does not interfere with the performance of your duties.

• does not take priority over your work responsibilities.

• does not cause unwarranted expense or liability to be incurred by the Company or our clients. •

does not have a negative impact on our business in any way; and

• is lawful and complies with this policy.

d) The Company will not tolerate the use of the E-mail system for unofficial or inappropriate purposes, including:

(i) any messages that could constitute bullying, harassment, or other detriment.

(ii) on-line gambling.

(iii) accessing or transmitting pornography.

(iv) transmitting copyright information and/or any software available to the user; or

(v) posting confidential information about other employees, the Company or its customers or suppliers.

D) USE OF INTERNET AND INTRANET

1) We trust you to use the internet sensibly. Although internet facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with and your use of the internet does not interfere in any way with the performance of your duties.

2) Whenever you access a web site, you should always comply with the terms and conditions governing its use. Care must be taken in the use of information accessed through the Internet. Most information is unregulated, and as such there is no guarantee of accuracy.

3) The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work related, leaves an individual liable to disciplinary action which could lead to dismissal.

4) You must not:

a) use any images, text or material which are copyright-protected, other than in accordance with the terms of the license under which you were permitted to download them.

b) introduce packet-sniffing or password-detecting software.

c) seek to gain access to restricted areas of the Company's network.

d) access or try to access data which you know or ought to know is confidential.

e) introduce any form of computer virus; nor

f) carry out any hacking activities.

E) VIRUS PROTECTION PROCEDURES

In order to prevent the introduction of virus contamination into the software system the following must be observed: -

a) unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used; and

b) all software must be virus checked using standard testing procedures before being used.

F) USE OF COMPUTER EQUIPMENT

To control the use of the Company's computer equipment and reduce the risk of contamination the following will apply:

a) The introduction of new software must first be checked and authorised by a member of management or a client's nominated senior member of management before general use will be permitted.

b) Only authorised staff should have access to the Company's computer equipment.

c) Only authorised software may be used on any of the Company's computer equipment.

d) Only software that is used for business applications may be used.

e) No software may be brought onto or taken from the Company's premises without prior authorisation.

f) Unauthorised access to the computer facility will result in disciplinary action.

g) Unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.

G) SYSTEM SECURITY

1) Security of our or our clients' IT systems is of paramount importance. We owe a duty to all our customers/clients to ensure that all of our business transactions are kept confidential. If at any time we need to rely in court on any information which has been stored or processed using our IT systems, it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.

2) The Company's system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.

3) Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

H) WORKING REMOTELY

1) This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and to your use of your own computer equipment or other computer equipment (e.g. client's equipment) whenever you are working on Company business away from our premises (working remotely).

2) When you are working remotely you must:

a) passwords protect any work which relates to our business so that no other person can access your work;

b) position yourself so that your work cannot be overlooked by any other person.

c) take reasonable precautions to safeguard the security of our laptop computers and any computer equipment on which you do Company business, and keep your passwords secret.

d) inform the police and the Company as soon as possible if either a Company laptop in your possession or any computer equipment on which you do our work has been stolen; and

e) ensure that any work which you do remotely is saved on the Company system or is transferred to our system as soon as reasonably practicable.

3) PDAs or similar hand-held devices are easily stolen and not very secure so you must password-protect access to any such devices used by you on which is stored any personal data of which the Company is a data controller or any information relating our business, our clients, or their business.

I) PERSONAL TELEPHONE CALLS/ MOBILE PHONES

1) Telephones are essential for our business. Incoming/outgoing personal telephone calls are allowed at the Company's head office but should be kept to a minimum. We reserve the right to recharge for excessive personal use. When visiting or working on client premises you should always seek permission before using our clients' telephone facilities.

2) Personal mobile phones should be switched off or 'on silent' during working hours and only used during authorised breaks.

J) MONITORING OF COMMUNICATIONS BY THE COMPANY

1) The Company is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy. The Company may monitor your business communications for reasons which include:

a) providing evidence of business transactions.

b) ensuring that our business procedures, policies and contracts with staff are adhered to.

c) complying with any legal obligations.

d) monitoring standards of service, staff performance, and for staff training.

e) preventing or detecting unauthorised use of our communications systems or criminal activities; and

f) maintaining the effective operation of Company communication systems.

2) From time to time the Company may monitor telephone, e-mail, and internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications). This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

3) Sometimes it is necessary for us to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday.

K) DATA PROTECTION

1) As an employee using our communications facilities, you will inevitably be involved in processing personal data for the Company as part of your job. Data protection is about the privacy of individuals and is governed by the General Data Protection Regulation and current Data Protection Act.

2) Whenever and wherever you are processing personal data for the Company you must keep this secret, confidential and secure, and you must take particular care not to disclose such data to any other person (whether inside or outside the Company) unless authorised to do so. Do not use any such personal data except as authorised by us for the purposes of your job. If in doubt, ask a member of management.

3) The Act gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an e-mail or otherwise. It is another reason why personal remarks and opinions made should be given responsibly, must be relevant and appropriate as well as accurate and justifiable.

4) For your information, the Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of the Company: you exceed your authority in collecting personal data; you access personal data held by us; or you pass them on to someone else (whether inside or outside the Company).

L) USE OF SOCIAL NETWORKING SITES

Any work-related issue or material that could identify an individual who is a customer/client or work colleague, which could adversely affect the company a customer/client or our relationship with any customer/client must not be placed on a social networking site. This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment, mobile phone, or PDA.

M) CONFIDENTIALITY

Employees are not permitted to register with sites or electronic services in the company's name without the prior permission of their manager. They are not permitted to reveal internal company information to any sites, be it confidential or otherwise, or comment on company matters, even if this is during after-hours or personal use. The company confidentiality policy applies to all electronic communication and data.

N) COMPLIANCE WITH THIS POLICY

1) Failure to comply with this policy may result in disciplinary action being taken against you. If there is anything in this policy that you do not understand, please discuss it with a member of management.

2) Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time.

Annex H

SUBJECT ACCESS REQUEST POLICY

A) AIM

You have a right, under the General Data Protection Regulation, to access the personal data we hold on to you. To do so, you should make a subject access request, and this policy sets out how you should make a request, and our actions upon receiving the request.

B) DEFINITIONS

"Personal data" is any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier, including your name.

"Special categories of personal data" includes information relating to:

a) race
b) ethnic origin
c) politics
d) religion
e) trade union membership
f) genetics
g) biometrics (where used for ID purposes)
h) health
i) sex life or
j) sexual orientation.

C) MAKING A REQUEST

Although subject access requests may be made verbally, we would advise that a request may be dealt with more efficiently and effectively if it is made in writing. If you wish to make a request, please use the Subject Access Request form.

Requests that are made directly by you should be accompanied by evidence of your identity. If this is not provided, we may contact you to ask that such evidence be forwarded before we comply with the request.

Requests made in relation to your data from a third party should be accompanied by evidence that the third party is able to act on your behalf. If this is not provided, we may contact the third party to ask that such evidence be forwarded before we comply with the request.

D) TIMESCALES

Usually, we will comply with your request without delay and at the latest within one month. Where requests are complex or numerous, we may contact you to inform you that an extension

of time is required. The maximum extension period is two months.

E) FEE

We will normally comply with your request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact you requesting a fee. This fee must be paid for us to comply with the request. The fee will be determined at the relevant time and will be set at a level which is reasonable in the circumstances.

In addition, we may also charge a reasonable fee if you request further copies of the same information.

F) INFORMATION YOU WILL RECEIVE

When you make a subject access request, you will be informed of:

a) whether or not your data is processed and the reasons for the processing of your data.
b) the categories of personal data concerning you.
c) where your data has been collected from if it was not collected from you. d) anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards utilised to ensure data security. e) how long your data is kept for (or how that period is decided);
f) your rights in relation to data rectification, erasure, restriction of and objection to processing.
g) your right to complain to the Information Commissioner if you are of the opinion that your rights have been infringed.
h) the reasoning behind any automated decisions taken about you.

G) CIRCUMSTANCES IN WHICH YOUR REQUEST MAY BE REFUSED

We may refuse to deal with your subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse your request, we will contact you without undue delay, and at the latest within one month of receipt, to inform you of this and to provide an explanation. You will be informed of your right to complain to the Information Commissioner and to a judicial remedy.

We may also refuse to deal with your request, or part of it, because of the types of information requested. For example, information which is subject to legal privilege or relates to management planning is not required to be disclosed. Where this is the case, we will inform you that your request cannot be complied with, and an explanation of the reason will be provided.

Annex J

Variation to terms and conditions (Document 6)

Important information about changes to your current employment documentation due to the introduction of new data protection laws

The General Data Protection Regulation (GDPR) will come into force in the UK on 25th May 2018 through a new Data Protection Act. We are committed to the principles of data security outlined in the GDPR and ensuring our compliance with our data protection obligations.

We have set out below some changes that are required because of the new laws, including a set of new policies that will come into effect on 25th May 2018.

Changes to your employment documentation

We have reviewed our current position in relation to GDPR and have identified new policies which are needed, or which must replace existing ones. This law, and the UK's own new Data Protection Act, will replace current data protection laws. Therefore, any references to the Data Protection Act 1998 in your current contractual documentation are, by way of this document, replaced with a reference to the General Data Protection Regulation and the Data Protection Act in force from time to time.

Our new policies are set out below and will come into effect from 25th May 2018:

- Data protection policy
- Communications policy
- Policy on your rights in relation to your data
- Data breach notification policy
- Subject access request policy

We have also implemented new privacy notices to be effective from 25th May 2018, which set out what personal data we use and how we use it:

- Privacy notice for employees
- Privacy notice for job applicants

Changes to your current Employee Handbook/Statement of Main Terms of Employment

1. The following clause in your employee handbook, 'DATA PROTECTION ACT 1998' is, with effect from 25th May 2018, replaced with:

DATA PROTECTION

The General Data Protection Regulation (GDPR) and the current Data Protection Act regulate our use of your personal data. As an employer it is our responsibility to ensure that the personal data we process in relation to you is done so in accordance with the required principles. Any data held shall be processed

fairly and lawfully and in accordance with the rights of data subjects.

We will process data in line with our privacy notices in relation to both job applicants and employees. You have several rights in relation to your data. More information about these rights is available in our "Policy on your rights in relation to your data". We commit to ensuring that your rights are upheld in accordance with the law and have appropriate mechanisms for dealing with such.

We may ask for your consent for processing certain types of personal data. In these circumstances, you will be fully informed as to the personal data we wish to process and the reason for the processing. You may choose to provide or withhold your consent. Once consent is provided, you can withdraw consent at any time.

You are required to comply with all company policies and procedures in relation to processing data. Failure to do so may result in disciplinary action up to and including dismissal.

2. The following clause in your employee handbook, 'THIRD PARTY INVOLVEMENT' is, with effect from 25th May 2018, replaced with:

THIRD PARTY INVOLVEMENT

We reserve the right to allow third parties to chair any meeting, for example disciplinary, capability, grievance, this is not an exhaustive list. We will seek your consent at the relevant time to share relevant 'special categories of data' where it is necessary for the purposes of that hearing.

3. The following clauses in your employee handbook, 'DISCLOSURE AND BARRING CERTIFICATES', and 'POLICY STATEMENT ON THE SECURE STORAGE, HANDLING, USE, RETENTION AND DISPOSAL OF DISCLOSURES AND DISCLOSURE INFORMATION' are, with effect from 25th May 2018, replaced with:

DISCLOSURE AND BARRING CERTIFICATE(S)

Your initial employment is conditional upon the provision of a satisfactory Disclosure and Barring Certificate of a level appropriate to your post. You may be required to undertake to subsequent criminal record checks from time to time during your employment as deemed appropriate by the Company. If such certificate(s) are not supplied your employment with us will be terminated.

POLICY STATEMENT ON THE SECURE STORAGE, HANDLING, USE, RETENTION AND DISPOSAL OF DISCLOSURES AND DISCLOSURE INFORMATION

During your employment, you are required to immediately report to the Company any convictions or offences with which you are charged, including traffic offences.

1) As an organisation using the Disclosure and Barring Service and/or Disclosure Scotland to help assess the suitability of applicants for positions of trust, we comply fully with the Disclosure and Barring Service/Disclosure Scotland Code of Practice regarding the correct handling, use, storage, retention and disposal of disclosures and disclosure information. We also comply fully with our obligations under the Data Protection Act.

2) Disclosure information is never kept in an applicant's personnel file. It is always kept separately and securely in lockable, non-portable storage containers with access strictly controlled and limited to those who are authorised to see it as part of their duties in accordance with Section 124 of the Police Act 1997.

3) We maintain a record of all those to whom disclosures and disclosure information has been revealed

and we recognise that it is a criminal offence to pass the information to anyone who is not entitled to receive it.

4) Disclosure information is only used for the specific purpose for which it was requested.

5) Once a recruitment (or other relevant) decision has been made, we do not keep disclosure information for any longer than is necessary to allow for the consideration and resolution of any disputes or complaints. Where appropriate, the Disclosure and Barring Service/Disclosure Scotland will be consulted, and full consideration will be given to the data protection and human rights of the individual.

6) Once the retention period has elapsed, we will ensure that any disclosure information is immediately destroyed by secure means, i.e. by shredding, pulping, or burning. While awaiting destruction, disclosure information will not be kept in any insecure receptacle (e.g. a waste bin or confidential waste sack). We will not keep any photocopy or other image of the disclosure or any copy or representation of the contents of the disclosure. However, we may keep a record of the date of issue of the disclosure, the name of the subject, the type of disclosure requested, the post for which the disclosure was requested, the unique reference number of the disclosure and the details of the recruitment (or other relevant) decision taken.

4. The clause entitled 'Monitoring' in the Email and Internet Policy is, with effect from 25th May 2018, amended as follows:

We reserve the right to monitor all e-mail/internet activity by you for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

5. Any reference to the term "sensitive data" contained in your employment documentation is, with effect from 25th May 2018, replaced with "special categories of data".

Data Protection Policy

A) INTRODUCTION

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded, and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers, and self-employed contractors. These are referred to in this policy as relevant individuals.

B) DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

C) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent.
b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing.
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay

e) data is not kept for longer than is necessary for its given purpose

f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.
g) we will comply with the relevant GDPR procedures for international transferring of personal data

D) TYPES OF DATA HELD

We keep several categories of personal data on our employees to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc.
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:

i) job title and job descriptions
ii) your salary
iii) your wider terms and conditions of employment
iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal, and performance information
v) internal and external training modules undertaken

All the above information is required for our processing activities. More information on those processing activities is included in our privacy notice for employees, which is available from your manager.

E) EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on to you:

a) the right to be informed about the data we hold on to you and what we do with it; b) the right of access to the data we hold on to you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';

g) the right to object to the inclusion of any information.
h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

F) RESPONSIBILITIES

To protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

G) LAWFUL BASES OF PROCESSING

We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the employee's consent to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed, and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

H) ACCESS TO DATA

As stated above, employees have a right to access the personal data that we hold on them. To exercise this right, employees should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

I) DATA DISCLOSURES

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a) any employee benefits operated by third parties.
b) disabled individuals - whether any reasonable adjustments are required to assist them at work;
c) individuals' health data - to comply with health and safety or occupational health obligations towards the employee.
d) for Statutory Sick Pay purposes.

e) HR management and administration - to consider how an individual's health affects his or her ability to do their job.
f) the smooth operation of any employee insurance policies or pension plans. g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

J) DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe. Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted. c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

K) THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures to maintain the Company's commitment to protecting data.

L) INTERNATIONAL DATA TRANSFERS

The Company does not transfer personal data to any recipients outside of the EEA.

M) REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

N) TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach. The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

O) RECORDS

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

P) DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Jack Greenwood

jack@v1ce.co