DATA PROTECTION AND IT SECURITY

1. VERSION CONTROL

Issue Date:	**20/10/23**	**Review Date:**	**20/10/23**
Change Control: General review, contents and paragraph numbering			
Version:	**1**	**Issued By:**	**P Hansford**

2. TABLE OF CONTENTS

3. INTRODUCTION

J.V. Barrett & Co. Ltd is a company registered in England under company number 1225448. Our registered office is ST Ivel Way, Warmley, Bristol, BS30 8TY. Data Protection and IT Security are key components of J.V. Barrett & Co. Ltd overall business management framework, and this document provides the framework for the more detailed information including policies and guidance for Data Protection, use of Data and IT Security.

These documents are applicable to all:

- J.V. Barrett & Co. Ltd group companies.
- Employees.
- Sub-contractors, suppliers, Instructors, Assessors, and other people working (paid or unpaid) on behalf of the company.

The Company takes compliance with these policies very seriously. Any breach of this policy or any breach of the data protection legislation will be regarded as misconduct and will be dealt with under the Company's disciplinary procedure.

4. COMMERCIAL DATA PROTECTION POLICY

Revision: 20/10/2023

4.1 PRIVACY STATEMENT

- J.V. Barrett & Co Ltd is committed to protecting the privacy of your personal data collected in the course of our business, including via the website www.barrettine.co.uk (the "Site"). This Data Processing Policy forms part of our Terms and Conditions of trade as well as part of the terms and conditions for use of and access to the Site.
- We as a business are dedicated to the improvement of working and social standards within the field of Chemical Manufacture & Distribution based at Warmley, Bristol. See Contact us section for further details.
- We comply and with relevant "Data Protection Legislations" where Data Protection Legislations includes the UK Data Protection Act 2018 ("DPA") and UK General Data Protection Regulation ("GDPR") as applicable, when processing your personal data.
- For the purposes of Data Protection Legislations, we will be the "data controller" of all personal data held in respect of this Policy. This means we determine the purpose and means of processing personal data.
- Our Data Protection Manager can be contacted at Warmley, Bristol Tel: 0117 9600060, or email: dataprotection@barrettine.co.uk.

4.2 DATA PROCESSING

4.2.1. In this Policy we use certain terms from the relevant data protection legislation.

- "Data subject" i.e., anyone who can be identified from personal data.
- "controller/data controller" i.e., a business which holds personal data and decides how it should be processed.
- "processor/data processor" i.e., a business which holds personal data on behalf of a controller and processes it in accordance with the controller's instructions.
- "Personal data" i.e., recorded information we hold about you from which you can be identified. It may include contact details, other personal information, photographs, expressions of opinion about you or indications as to our intentions about you.
- "processing" i.e., doing anything with personal data including collecting, using, storing, accessing, disclosing, and destroying it.

4.2.2. We will process your personal data in accordance with the following principles:

- all personal data must be processed lawfully, fairly and in a transparent manner.
- all personal data must be collected for one or more specified, explicit, and legitimate purposes and not processed in a manner incompatible with those purposes.
- all personal data shall be restricted to what is adequate, relevant, and limited for those purposes.
- all personal data shall be kept accurate and up to date and reasonable steps must be taken to erase or rectify inaccurate personal data.
- all personal data must be kept for no longer than is necessary for those purposes.
- all personal data must be protected by appropriate technical and organisational security measures to prevent unauthorised or unlawful processing and accidental loss, destruction, or damage.

4.2.3 This Policy applies to the processing of personal data by us in connection with any:

- Customers: Organisations or persons for the provision of services by us.
- Suppliers: For the provision of products and services to us by our suppliers or service providers.
- Visitors: Where an individual is a visitor on our website.

4.3. TYPES OF PERSONAL DATA

Personal data or personal information means any information about an individual from which that person can be identified. It does not include data where the identity has been removed. This is known as anonymised data. Anonymised data falls outside the scope of Data Protection Legislations.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together:

- Identity Data includes first name, last name, username or similar identifier and title.
- Contact Data includes billing address, delivery address, email address and telephone numbers.
- Financial Data includes bank account and payment card details.
- Transaction Data includes details about payments to and from you and other details for the provision of services you have purchased from us.
- Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website.
- Profile Data includes your username and password, searches made by you, your ratings and comments, preferences, feedback, and survey responses.
- Usage Data includes information about how you use our website and services.
- Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

4.4. HOW WE COLLECT YOUR PERSONAL DATA

Directly from you: You give us your personal data in your direct interactions with us. Such personal data includes Identity Data, Contact Data, Financial Data, Profile Data, Usage Data, Technical Data, Marketing and Communications Data.

From use of our website: We gather information and statistics collectively about visitors to our website. Analysis of this information demonstrates the most frequently used sections of the website and assists us in continually improving the online service. You give us your personal data, which includes Profile Data, Usage Data, Technical Data and/or Marketing and Communications Data when you use our website or which we have agreed with you to use or when you review any publications or marketing material, we send you. Please see our Cookies Policy for more information.

Indirectly: Third-party sources: We can receive Identity Data and Contact Data about you from third parties when:

- we provide our services or other parties send us your personal data to enable the provision of those service.
- you provide your personal data to a third party for the purpose of sharing it with us.

4.5 LAWFUL BASIS OF PROCESSING

4.5.1 Where we need to collect personal data by law or under the terms of a contract we have with you, and you do not provide that information when requested we may not be able to perform the contract we have or are trying to enter into with you for example to provide you with our services. In this case we may have to cancel our services with you.

4.5.2 We may collect, use, and store your personal data, as described in this Policy where necessary in order to:

- perform any contract to which you are party or in order to take steps at your request prior to entering into a contract.
- exercise our legitimate business interests.
- carry out other functions with your specific consent; and
- comply with a legal obligation such as for our accounting, legal or regulatory purposes.

4.5.3. Purposes for which we will use your personal data.

We have set out below in a table format a description of all the ways we plan to use your personal data and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground, we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
For the provision of our services to you	(a) Identity (b) Contact	Performance of a contract with you
To respond to any enquires	(a) Identity (b) Contact	(a) Performance of a contract with you (b) Necessary for our legitimate interests
To process and deliver our services to you including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests i.e., to recover debts due to us
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy	(a) Identity (b) Contact (c) Profile	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation

(b) Asking you to leave a review or take a survey	(d) Marketing and Communications	(c) Necessary for our legitimate interests i.e., to keep our records updated and to study how customers use our products/services
To administer and protect our business and this website including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests i.e., to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy. Note: Where applicable consent will be used for data analytics obtained through cookies or similar technologies. See our Cookies Policy.
To make suggestions and recommendations to you about our services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications	Necessary for our legitimate interests to develop our products/services and grow our business

4.5.4. Marketing communications

We may send you marketing communication. You have the right to object to processing of your personal data for direct marketing purposes. You can unsubscribe from receiving marketing communications from us by using the unsubscribe methods contained in communications we send to you or by contacting us. See Contact us.

Where you unsubscribe out of receiving marketing communications this will not apply to personal data provided to us as a result of registering for or using our service, your service experience, or other interactions with this website. Please note requests to unsubscribe may take up to 28 days to be fully implemented.

4.6 SHARING PERSONAL DATA

4.6.1. We do not and will not sell any of your personal data to any third party including your name, contact information or payment information.

4.6.2. We may have to share your personal data with the parties set out below:

- Internally: Your personal data will be used by our employees and contractors who are working on providing your services to you on a need-to-know basis.
- Suppliers: This would include service providers who support our business including IT and communication suppliers and outsourced business support to ensure our service runs smoothly.
- Professional advisers: This would include lawyers, bankers, auditors, and insurers who provide consultancy, banking, legal, insurance and accounting services.
- Law enforcement bodies, regulators, and other authorities: This is to comply with our legal requirements or adhere to good practices.
- Advertising networks and analytics service providers: This is to support and display ads on our website and other social media tools.
- Third parties: This is in the context of the acquisition or transfer of any part of our business or in connection with the business reorganisation. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Policy.

4.7 INTERNATIONAL TRANSFERS

4.7.1. We may transfer and process your personal data outside of the United Kingdom to countries where data protection laws are less stringent than those in the UK. When we transfer your personal data outside of the UK, we only do so to entities that offer our users the same level of data protection as that afforded by the Data Protection Legislations.

- We will only transfer your personal information to countries that have been deemed to provide an adequate level of protection for personal information; or
- We will use specific contracts approved for use in the UK which give personal information the same protection it has in the UK. For example, the use of Article 46 UK GDPR safeguard mechanisms to transfer personal data endorsed by the UK Government.

To find out more about the transfer mechanism used please contact us.

4.8 DATA SECURITY

4.8.1. We have implemented generally accepted standards of technology and operational security in order to protect personal data from loss, misuse, or unauthorised alteration or destruction. We will notify you promptly in the event of any breach of your personal data which might expose you to serious risk.

4.9 DATA RETENTION

4.9.1 We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

4.9.2 To determine the appropriate retention period for personal information we consider the amount, nature and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means and the applicable legal, regulatory, tax, accounting, or other requirements.

4.9.3 We will hold your personal data on our systems for as long as:

- your account remains valid; and/or
- any contracts you make with us are live; and/or
- is necessary to comply with our legitimate business interests; and/or
- is necessary to comply with our legal obligations; and/or
- you have indicated you are happy for us to do so.

4.9.4 We may anonymise your personal data so that it can no longer be associated with you for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

4.10 DATA SUBJECT RIGHTS

4.10.1 Under certain circumstances, you have rights under Data Protection Legislations. Not all rights are absolute. You can:

Request access to your personal data: This is known as a "data subject access request" and enables you to receive a copy of the personal data we hold about you.

Request correction of your personal data: This enables you to have any incomplete or inaccurate information we hold about you corrected.

Request erasure of your personal data: This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. Note: We may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you at the time of your request.

Object to processing of your personal data: This is where we are processing your personal data based on a legitimate interest or those of a third party and you may challenge this. However, we may be entitled to continue processing your information based on our legitimate interests or where this is relevant to any legal claims.

See also Marketing communications.

Request restriction of processing your personal information: This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the information's accuracy (b) where our use of the information is unlawful, but you do not want us to erase it (c) where you need us to hold the information even if we no longer require it as you need it to establish, exercise or defend legal claims or (d) you have objected to our use of your information, but we need to verify whether we have overriding legitimate grounds to use it.

Request transfer of your personal information (“data portability”): This is where in some circumstances we will provide to you or a third party you have chosen your personal data in a structured, commonly used, machine-readable format.

Right to withdraw consent: This is where we are relying on consent to process your personal data. This will not affect the lawfulness of any processing carried out before you withdraw your consent.

Depending on the processing activity, if you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

Automated decision making: This is where decisions are made about you by automated means. We do not carry out automated decision making.

4.10.2 Carrying out your data subject rights.

You will not have to pay a fee to access your personal data or to exercise any of the other rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal information or to exercise any of your other rights. This is a security measure to ensure that personal information is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

If you wish to exercise any of the rights set out above, please contact us.

4.11 CONCERNS AND COMPLAINTS

4.11.1 If you consider that we have not complied with this Policy or the relevant data protection legislation in respect of your personal data or someone else's, you should raise the matter with our Data Protection Manager. Any such breach will be taken seriously and will be dealt with in accordance with the relevant Data protection Legislations.

4.11.2 You have the right to take any complaints about how we process your personal data to the Information Commissioner: Information Commissioner's Office, Wycliffe House. Water Lane. Wilmslow. Cheshire SK9 5AF. Email: https://ico.org.uk/concerns/ Tel: 0303 123 1113.

4.12 CHANGES TO OUR POLICY

4.12.1 This Policy may be changed from time to time in response to legal, technical, or business developments. We will take appropriate measures to inform you when we update our Policy. We will obtain your consent to any material Policy changes if and where this is required by applicable Data Protection Legislations.

4.13. CONTACT US

4.13.1 For more details, please consult the relevant Data Protection Legislations or address any questions, comments to our Data Protection Manager on Tel: 0117 9600060 or on email at dataprotection@barrettine.co.uk

4.14 LINKS TO OTHER WEBSITES

4.14.1 The Site may from time to time contain links to other unrelated sites (including those of our advertisers). This privacy statement does not apply to these sites nor are we responsible for the content and practices of these websites. In particular, please note that such other sites may also use cookies, and that we have no control over this. Please refer to our Cookie Policy.

4.15 VERSION CONTROL

4.15.1 This version was last updated on 20 October 2023.

DATA RETENTION POLICY

5.1 RETENTION AND DESTRUCTION OF DATA

5.1.1 J.V. Barrett & Co. Ltd of St Ivel Way, Warmley, Bristol, BS30 8TY is committed to protecting the privacy of all personal data collected in the course of our business. We will at all times ensure that the minimum amount of personal data is kept, and for no longer than necessary, for us to meet our document retention objectives and data protection obligations.

5.1.2 This Data Retention Policy sets out how we will store and delete personal data and is an important part of our data protection compliance processes. It should be read alongside our Data Protection Policy, of which it forms a part.

5.1.3 In the course of carrying out our various functions, we may collect, use, store, access, disclose and destroy information relating to individuals. This information may originate with those individuals or third parties or be generated by us.

5.1.4 In certain circumstances, it will be necessary to retain specific information (as well as the files or documents which contain such information) in order to fulfil our contractual, statutory or regulatory requirements and/or to meet our operational needs. Document retention may also be useful to evidence events or agreements in the case of disputes or to preserve information which has historic value.

5.1.5 Premature destruction or inappropriate retention of documents could result in our inability to defend litigious claims, deal with operational difficulties or failure to comply with the Data Protection Act 2018 ("DPA"), UK General Data Protection Regulation ("GDPR") or other applicable data protection legislation.

5.1.6 Furthermore, large-scale retention of documents and records is impractical and appropriate disposal is encouraged. Disposal will assist us to maintain sufficient electronic and office storage space and will de-clutter physical office space, resulting in a safer and more effective working environment.

5.1.7 It is therefore important for us to have in place systems for the timely and secure disposal of documents and records that are no longer required for business purposes.

5.2 SCOPE OF POLICY

5.2.1 This Policy applies to all our employees, contractors and agents who use our network and computer systems to process personal data. This Policy also applies to paper records.

5.2.2 Failure to comply with this Policy is a serious matter and may lead to disciplinary action up to and including discharge.

5.2.3 This Policy does not override or replace any obligation we may owe to any party (or vice versa) in respect of confidential information. Confidential information should not be processed in breach of any such obligation, whether or not subject to any confidentiality agreement or non-disclosure agreement. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted.

5.2.4 All breaches of this Policy should be reported to the Data Protection Manager, Andy Heath at St Ivel Way, Warmley, Bristol, BS30 8TY to whom all queries regarding this Policy should also be addressed.

5.2.5 Our records must be stored in a safe, secure, and accessible manner. All electronic documents and files that are essential to our business operations must be duplicated and/or backed.

5.2.6 Our Data Protection Manager is responsible for the continuing process of identifying which records and information have met their required retention period and for supervising their destruction.

5.2.7 Physical confidential, financial, and personnel-related records must be destroyed by shredding where possible. Other physical records may be destroyed by secure recycling.

5.2.8 Where not retained subject to appropriate anonymisation or pseudonymisation, digital records must be destroyed by irreversible overwriting.

6. PERSONNEL DATA PROTECTION POLICY

6.1 PURPOSE

The purpose of this policy is to set out what we expect from you and to ensure that you understand and comply with the rules governing the processing of personal data to which you may have access in the course of your work, so as to ensure that neither the Company nor you breach the data protection legislation.

This policy applies to all members of staff. It is non-contractual and does not form part of any employment contract, casual worker agreement.

6.2 DEFINITIONS

In this policy, the following words and phrases have the following meanings:

"Consent" means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

"Data protection legislation" means the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any other applicable primary or secondary legislation as may be in force in the UK from time to time.

"Data subject" means a living identified or identifiable individual about whom the Company holds personal data.

"Member of staff" is any director, employee, worker, agency worker, apprentice, intern, volunteer, contractor, and consultant employed or engaged by the Company.

"Personal data" is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or 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 data subject. It excludes anonymised data, i.e., where all identifying particulars have been removed.

"Processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing, or destroying. It also includes transmitting or transferring personal data to third parties.

6.3 THE DATA PROTECTION PRINCIPLES

Under the data protection legislation, there are six data protection principles that the Company and all members of staff must comply with at all times in their personal data processing activities. In brief, the principles say that personal data must be:

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

6.3.2 Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

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

6.3.4 Accurate and, where necessary, kept up to date; every reasonable step must also 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).

6.3.5 Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (storage limitation).

6.3.6 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).

The Company is responsible for, and must be able to demonstrate compliance with, these data protection principles.

6.4 YOUR OBLIGATIONS IN RELATION TO PERSONAL DATA

The Company takes compliance with data protection policy very seriously. Any breach of this policy or any breach of the data protection legislation will be regarded as misconduct and will be dealt with under the Company's disciplinary procedure. A significant or deliberate breach of this policy, such as accessing a data subject's personal data without authority or unlawfully obtaining or disclosing a data subject's personal data (or procuring their disclosure to a third party) without the Company's consent, constitutes a gross misconduct offence and could lead to your summary dismissal.

You must comply with this policy and the data protection principles at all times in your personal data processing activities where you are acting on behalf of the Company in the proper performance of your job duties and responsibilities. We rely on you to help us meet our data protection obligations to data subjects.

Under the data protection legislation, you should also be aware that you are personally accountable for your actions, and you can be held criminally liable. It is a criminal offence for you knowingly or recklessly to obtain or disclose personal data (or to procure their disclosure to a third party) without the consent of the Company. This would include, for example, taking clients' or customers' contact details or other personal data without the Company's consent on the termination of your employment, accessing another employee's personal data without authority or otherwise misusing or stealing personal data held by the Company.

Where unlawful activity is suspected, the Company will report the matter to the Information Commissioner's Office for investigation into the alleged breach of the data protection legislation and this may result in criminal proceedings being instigated against you. This conduct would also amount to a gross misconduct offence under the Company's disciplinary procedure and could

lead to your summary dismissal.

Lawfulness, fairness, transparency

Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, process, and share personal data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process personal data fairly and without adversely affecting the Data Subject.

The UK GDPR allows processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her consent.
- the processing is necessary for the performance of a contract with the Data Subject.
- to meet our legal compliance obligations.
- to protect the Data Subject's vital interests.
- to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

6.5 CONSENT

As a controller we must only process personal data on the basis of one or more of the lawful bases set out in the UK GDPR which include consent.

A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

We must evidence consent captured and keep records of all consents in accordance with related policies and privacy guidelines so that we can demonstrate compliance with consent requirements.

6.6 TRANSPARENCY (notifying Data Subjects)

The UK GDPR requires us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The 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 them.

Whenever we collect personal data directly from Data Subjects, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the controller as to how and why we will use, process, disclose, protect, and retain that personal data through a privacy notice which must be presented when the Data Subject first provides the personal data.

When personal data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the personal data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed processing of that personal data.

6.7 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 use personal data for new, different, or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

6.8 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 may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties. You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with Barrettine Group data retention guidelines.

6.9 ACCURACY

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. You will ensure that the personal data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

6.10 STORAGE LIMITATION

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held unless a law requires that data to be kept for a minimum time. You must comply with Barrettine Group Data Retention Policy.

We must not keep personal data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

We will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable. We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice(s).

6.11 SECURITY INTEGRITY AND CONFIDENTIALITY

Protecting personal data

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

We develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. You are responsible for protecting the personal data we hold.

You must follow 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 may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the personal data defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
- Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

You must comply with the following security measures at all times:

- only access personal data that you have authority to access and only for authorised purposes, e.g., if you need them for the work you do for the Company, and then only use the data for the specified lawful purpose for which they were obtained.
- only allow other members of staff to access personal data if they have the appropriate authorisation and never share personal data informally.
- do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Company's website or posted on the Internet in any form unless the data subject has given their explicit consent to this.
- be aware that those seeking personal data sometimes use deception to gain access to them, so always verify the identity of the data subject and the legitimacy of the request.
- where the Company provides you with code words or passwords to be used before releasing personal data, you must strictly follow the Company's requirements in this regard.
- only transmit personal data between locations by e-mail if a secure network is in place, e.g., encryption is used for e-mail.
- if you receive a request for personal data about another member of staff or data subject, you should forward this to the Company's Data Protection Manager.
- ensure any personal data you hold are kept securely, either in a locked non-portable filing cabinet or drawer if in hard copy, or password protected or encrypted if in electronic format, and comply with Company rules on computer access and secure file storage.
- do not access another member of staff's personal data, e.g., their personnel records, without authority as this will be treated as gross misconduct and it is a criminal offence.
- do not obtain or disclose personal data (or procure their disclosure to a third party) without authority or without the Company's consent as this will be treated as gross misconduct and it is a criminal offence.
- do not remove personal data, or devices containing personal data, from the workplace with the intention of processing them elsewhere unless this is necessary to enable you to properly carry out your job duties and responsibilities, you have adopted appropriate security measures (such as password protection or encryption) to secure the data and the device, and it has been authorised by your line manager.
- ensure that, when working on personal data as part of your job duties and responsibilities when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security.

- do not store personal data on local computer drives, your own personal computer or on other personal devices.
- do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g., by shredding hard copies.
- remember that compliance with the data protection legislation and the terms of this policy is your personal responsibility.

6.12 REPORTING A PERSONAL DATA BREACH.

The UK requires controllers to notify any personal data breach to the Information Commissioner and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected personal data breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact your line manager.

6.13 TRANSFER LIMITATION

The UK restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. We may only transfer personal data outside the UK if one of the following conditions applies:

- the UK/EU has issued regulations confirming that the country to which we transfer the personal data ensures an adequate level of protection for the Data Subject's rights and freedoms.
- appropriate safeguards are in place such as standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism.
- the Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks.
- the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

6.14 DATA SUBJECTS RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their personal data. These include rights to:

- withdraw consent to processing at any time.
- receive certain information about our processing activities.
- request access to their personal data that we hold.
- prevent our use of their personal data for direct marketing purposes.

- ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.
- restrict processing in specific circumstances.
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest.
- request a copy of an agreement under which personal data is transferred outside of the UK.
- object to decisions based solely on Automated Processing including profiling (ADM).
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else.
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
- make a complaint to the supervisory authority.
- 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.

We must verify the identity of an individual requesting data under any of the rights listed above and do not allow third parties to persuade you into disclosing personal data without proper authorisation. You must immediately forward any Data Subject request you receive to the Data Protection Manager.

6.15 ACCOUNTABILITY

We as a business must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for and must be able to demonstrate compliance with the data protection principles.

We must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- appointing a suitably qualified DPO or equivalent where necessary and an executive accountable for data privacy.
- implementing Privacy by Design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects.
- integrating data protection into internal documents including this Policy, related policies, privacy guidelines or privacy notices.
- providing training on the UK GDPR.
- 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.

6.16 RECORD KEEPING

The UK GDPR requires us to keep full and accurate records of all our data processing activities. We must keep and maintain accurate corporate records reflecting our processing including

records of Data Subjects' consents and procedures for obtaining consents in accordance with any Company's record-keeping guidelines.

6.17 TRAINING AND AUDIT

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with the Company's mandatory training guidelines. You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

6.18 PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

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 privacy principles.

We must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that process personal data by taking into account the following:

- the state of the art.
- the cost of implementation.
- the nature, scope, context, and purposes of processing.
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.
- We must also conduct DPIAs in respect to high-risk processing.
- We should conduct a DPIA and discuss your findings with the Data Protection Manager when implementing major system or business change programs involving the processing of personal data including:
- use of new technologies (programs, systems, or processes), or changing technologies (programs, systems, or processes).
- Automated Processing including profiling and ADM.
- large-scale, systematic monitoring of a publicly accessible area.

You must comply with any of our guidelines on DPIA and Privacy by Design.

6.19 DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers.

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 products or 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 customer 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.

You must comply with any Company's guidelines on direct marketing to customers.

6.20 SHARING PERSONAL DATA

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the personal data we hold with another employee, agent or representative of our group which includes our subsidiaries and our ultimate holding company along with its subsidiaries if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

7. CHANGES TO THIS POLICY

The Company will review this policy at regular intervals and we reserve the right to update or amend it at any time and from time to time. We will circulate any modified policy to members of staff and, where appropriate, we may notify you of changes by e-mail.

It is intended that this policy is fully compliant with the data protection legislation. However, if any conflict arises between the data protection legislation and this policy, the Company will comply with the data protection legislation.

This policy may also be made available to the Information Commissioner’s Office on request.

8. TYPES OF PERSONAL DATA AND SECURITY

	Location						
	(a) Hard Copies - Secure Kept in Board Room	(b) Company Secure Servers	(c) Line Manger Secure	(d) Emergency Information	(e) Hard Copies - Secure BEH	(f) Hard Copies - Secure Sales Office Use	(g) General Filing
Employee							
Contact Details	y	y					
Date of Birth	y	y					
Training Certificates	y						
Qualifications	y						
UK Right to Work Information	y						
Salary		y					
Financial Information		y					
Training assessments - written			y				
Appraisals, reviews, targets, objectives		y	y				
Disciplinary Information		y					
Medical History	y						
Criminal Convictions	y						
Employment contracts	y						
Holidays, sickness, absence			y				
Company Training Matrix Records							y
PPE issue/use							y
Respirator, Face Fitting details							y
Induction Training							y
Safety Training							y
Supplier							
Name		y	y	y			
Contact Details		y	y	y			
Bank Financial Details		y					
Safety Data Sheets			y	y			y
Emergency Contact Details			Y	y			y
Customer							
Name		y	y	y	y		
Contact Details		y	y	y	y		
Company Registration Number		y	y		y		
VAT Number		y	y		y		
Bank Financial Details		y					
CC Payment Details						y	
Website Login Details		y					
References		y					
Credit Checks		y					
Stewardship details		y			y		

(a) Hard Copies - Secure - Kept in Board Room

- Do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Company's website or posted on the Internet in any form, unless the data subject has given their explicit consent to this
- When not in use ensure personal data is kept securely in a locked non-portable filing cabinet or drawer.
- Do not obtain or disclose personal data to a third party without authority or without the Company's consent.
- Do not remove personal data from the workplace with the intention of processing them elsewhere.
- Do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g. by shredding hard copies.

(b) Company Secure Servers

- Do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Company's website or posted on the Internet in any form, unless the data subject has given their explicit consent to this.
- Ensure any personal data is password protected or encrypted, and comply with Company rules on computer access and secure file storage.
- Do not obtain or disclose personal data to a third party without authority or without the Company's consent.
- Do not remove personal data from the workplace with the intention of processing them elsewhere.
- Where the Company provides you with code words or passwords to be used before releasing personal data, you must strictly follow the Company's requirements in this regard.
- Only transmit personal data between locations by e-mail if a secure network is in place, e.g. encryption is used for e-mail.
- Do not store personal data on local computer drives, your own personal computer or on other personal devices.
- Do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g. by shredding hard copies.

(c) Line Manger Secure

- Do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Company's website or posted on the Internet in any form, unless the data subject has given their explicit consent to this.
- Ensure any personal data is password protected or encrypted, and comply with Company rules on computer access and secure file storage.
- When hard copies are not in use ensure personal data is kept securely in a locked non-portable filing cabinet or drawer.
- Do not obtain or disclose personal data to a third party without authority or without the Company's consent.
- Do not remove personal data from the workplace with the intention of processing them elsewhere.

- Where the Company provides you with code words or passwords to be used before releasing personal data, you must strictly follow the Company's requirements in this regard.
- Only transmit personal data between locations by e-mail if a secure network is in place, e.g. encryption is used for e-mail.
- Do not store personal data on local computer drives, your own personal computer or on other personal devices.
- Do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g. by shredding hard copies.

(d) Emergency Information

- When hard copies are not in use ensure personal data is kept securely in a locked non-portable filing cabinet or drawer.
- Do not obtain or disclose personal data to a third party without authority or without the Company's consent.

(e) Hard Copies - Secure BEH

- Do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Company's website or posted on the Internet in any form, unless the data subject has given their explicit consent to this
- When not in use ensure personal data is kept securely in a locked non-portable filing cabinet or drawer.
- Do not obtain or disclose personal data to a third party without authority or without the Company's consent.
- Do not remove personal data from the workplace with the intention of processing them elsewhere.
- Do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g. by shredding hard copies.

(f) Hard Copies - Secure Sales Office Use

- Do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Company's website or posted on the Internet in any form, unless the data subject has given their explicit consent to this
- Do not obtain or disclose personal data to a third party without authority or without the Company's consent.
- Do not remove personal data from the workplace with the intention of processing them elsewhere.
- Do not make copies of personal data and dispose by shredding hard copies.

(g) General Filing

- General office filing and easily retrievable.