Privacy Standard

This Privacy Standard sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties. This document, (together with Related Policies and guidance) is an internal document and should not be shared with third parties, clients or regulators without prior authorisation.

Date created:		Last reviewed:	

1. INTRODUCTION

1.1 This Privacy Standard ("Standard") sets out how we handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

1.2 The Standard applies to all Company Personnel (hereafter referred to interchangeably as "you" and "your").

1.3 You must read, understand and comply with this Standard when processing Personal Data on our behalf.

1.4 This Standard sets out what we expect from you in order for the Company to comply with the Data Protection Legislation. Your compliance with this Standard is mandatory. Other policies exist to help you interpret and act in accordance with the principles outlined in this document; these must also be complied with.

1.5 Any intentional or unreasonable breach of this Standard may result in disciplinary action.

1.6 Responsibility for the Company's Data Protection ultimately falls to the highest level of management, and in our organisation we have nominated a Data Protection Manager who is responsible for ensuring this policy is adhered to (also called the "Responsible Person"). They are:

Laura Humphrey, Partner, laura@humphreyandbrand.com

1.7 SCOPE

1.8 Humphrey and Brand Residential LLP ("The Company") recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and provide for successful business operations.

1.9 Protecting the confidentiality and integrity of Personal Data is a business-critical responsibility.

1.10 You must contact a Responsible Person if you have any concerns that this Standard is not being followed.

1.11 You should also seek advice from a Responsible Person in the following circumstances:

- **(a)** if you are unsure of the lawful basis for processing a particular category of Personal Data;
- **(b)** if you need to rely on Consent and/or need to capture Explicit Consent;
- **(c)** if you need to draft Privacy Notices;
- **(d)** if you are unsure about the retention period for the Personal Data being Processed;
- **(e)** if you are unsure about what security or other measures you need to implement to protect Personal Data;
- **(f)** if there has been a Personal Data Breach;
- **(g)** if you are unsure on what basis to transfer Personal Data outside the EEA;
- **(h)** if you need any assistance dealing with any rights invoked by a Data Subject;
- **(i)** whenever you are engaging in a significant new processing activity which is likely to require a Data Protection Impact Assessment;

(j) if you feel you have to use Personal Data for purposes others than what it was collected for;
(k) If you plan to undertake any activities involving Automated Processing;
(l) If you need help complying with applicable law when carrying out direct marketing activities;
(m) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties.

2. PERSONAL DATA PROTECTION PRINCIPLES

2.1 We adhere to these principles whenever we to process Personal Data:

- **Lawfulness, Fairness and Transparency**: The data is processed within the terms of the GDPR, fairly and in a manner which enables accountability and compliance with Data Protection rights.
- **Purpose Limitation:** The data is collected only for specified, explicit and legitimate purposes.
- **Data Minimisation:** The data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy:** The data is accurate and kept up to date where necessary.
- **Storage Limitation:** The data is not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed.
- **Security, Integrity and Confidentiality:** The data is Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- **Transfer Limitation:** The data is not transferred to any another country without appropriate safeguards being in place
- **Data Subjects' Rights and Requests:** The data is made available to Data Subjects and they are able and assisted in exercising certain rights in relation to their Personal Data.
- **Accountability:** We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

3. LAWFULNESS, FAIRNESS, TRANSPARENCY

3.1 Personal data must be processed lawfully, fairly and in a transparent manner with the involvement of the Data Subject.

3.2 You may only collect, process and share Personal Data fairly and lawfully and for specified purposes.

3.3 The GDPR restricts the processing of Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing, but to ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

3.4 Whenever we collect or process Personal Data we ensure it is necessary for one of the following reasons:

(a) to fulfil a contract with the Data Subject;
(b) to meet our legal compliance obligations;
(c) to protect the Data Subject's vital interests;
(d) to pursue our legitimate interests, which have been set out in a Privacy Notice to the Data Subject, and where the purpose for processing does not prejudice the interests or fundamental rights and freedoms of Data Subjects
(e) the Data Subject has given their Consent.

3.5 We identify and document the legal grounds for each of our processing activities.

4. CONSENT

4.1 When no other legal basis can be relied upon to process data that is necessary for our activities, we will seek the Consent of the Data Subject.

4.2 The conditions of a consent being genuine and lawful require that it fulfils the following criteria:

- **Freely-given:** The Data Subject must be able to choose whether they give their consent.

- **Unambiguous:** The consent must detail clearly the purpose or purposes of the processing in a format which is succinct, readable, and leaves no room for doubt over whether the Data Subject has fully understood and appreciated what they are consenting to. The consent must also be given with a positive indication from the Data Subject, such as a by giving their signature or ticking a box to 'opt in', but under no circumstances being asked to un-tick a pre-ticked box or be asked to 'opt out'.
- **Specific:** The consent must relate only to the personal data specified in the consent and for the purposes that are specified and contain an assurance that no other unspecified processing will take place.
- **Separate:** The Consent must be distinguishable from any other agreements the Data Subject is entering into and cannot be a pre-condition to any service being provided.
- **Informed:** The Data Subject must be given information about their rights under the Data Protection Legislation to guide their consent, and their rights in relation to access, erasure and withdrawing their 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.
- **Explicit:** In the case of Special Categories of Personal Data (a.k.a 'Sensitive Personal data'), processing must be for an explicit purpose and not for a general purpose, whether or not this has been specified. Examples include processing but not permanently storing health information to refer employees to an occupational health worker.

4.3 A request from a Data Subject to withdraw consent must be honoured immediately and withdrawing consent must be as easy as proving it.

4.4 If the purpose of processing a Data Subject's information changes at any time, to any purpose which the Data Subject has not consented to, the Consent will need to be refreshed by contacting the Data Subject.

4.5 Unless we have relied on another legal basis of processing, Explicit Consent is usually required for processing Sensitive Personal Data, for Automated Decision-Making and for cross-border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

4.6 We must be able to produce evidence of all the Consents we acquire to demonstrate our compliance with these requirements.

5. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

5.1 Data Controllers need to provide this information to Data Subjects at the point where data is collected:

- **Our** organisation name and the contact details of a Responsible Person.
- The purposes of the processing and lawful basis relied upon.
- Where the Personal Data was not supplied by the data subject: the categories of Personal Data and where it came from
- The recipient (or categories of recipients)
- The relevant retention period/s
- The Data Subject's rights
- Where applicable details of any statutory or contractual obligation to provide the data
- Details of any Automated Decision Making

5.2 This will be provided through appropriate Privacy Notices which will be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6. PURPOSE LIMITATION

6.1 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.

6.2 You cannot use Personal Data for new, different or incompatible purposes other than those disclosed when the data was first obtained unless you have informed the Data Subject of the new purposes and – if their consent is required – we have obtained that consent.

7. DATA MINIMISATION

7.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

7.2 You may only Process Personal Data when performing your job duties requires it.

7.3 You cannot Process Personal Data for any reason unrelated to your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

7.4 We will ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines and we require your assistance to ensure this objective is attained.

8. ACCURACY

8.1 Personal Data must be accurate and, where necessary, kept up to date.

8.2 When Personal Data is inaccurate It must be corrected or deleted without delay.

8.3 You will take reasonable steps to ensure that the Personal Data we process is accurate, complete, kept up to date and relevant to the purpose for which we collected it.

8.4 You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

8.5 You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. STORAGE LIMITATION

9.1 You 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.

9.2 You must comply with the Company's guidelines on Data Retention.

9.3 You will assist us by taking 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.

9.4 We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined by issuing a suitable Privacy Notice.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

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

10.2 We will 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.

10.3 We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data.

10.4 You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

10.5 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.

10.6 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.

10.7 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

10.8 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

11. REPORTING A PERSONAL DATA BREACH

11.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

11.2 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 required to do so.

11.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact a Responsible Person.

11.4 You should preserve all evidence relating to the potential Personal Data Breach.

12. TRANSFER LIMITATION

12.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

12.2 You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

12.3 You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO
- 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 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.

13. DATA SUBJECT RIGHTS AND REQUESTS

13.1 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 Personal Data 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
- Require us to rectify inaccurate data or to complete incomplete data
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest
- Object to decisions based solely on Automated Processing, including profiling and Automated Decision Making
- 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

13.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

13.3 You must immediately forward any Data Subject request you receive to a Responsible Person.

14. ACCOUNTABILITY

14.1 We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

14.2 We will ensure the following adequate resources and controls are in place to ensure, and to document, GDPR compliance:

- We will have a appointed Responsible Persons
- We will implement Privacy by Design when processing Personal Data
- We will complete DPIAs where processing presents a high risk to rights and freedoms of Data Subjects
- We specify our approach to data protection in internal documents including this Standard and other Polices
- We ensure Company Personnel are trained on the GDPR and maintain a record of training attendance
- We test the privacy measures implemented on a regular basis
- We conduct periodic reviews and audits to assess compliance

15. RECORD KEEPING

15.1 We will keep full and accurate records of all our data processing activities.

15.2 All Company Personnel must assist, where required, to keep and maintain accurate records.

15.3 These records will include such things as:

Our name and contact details [and those of our DPO]

- The categories of Personal Data
- The categories of Data Subject
- The processing activities / purposes
- Any third-party recipients of the Personal Data,
- The storage locations
- The retention periods
- A description of the security measures in place

16. TRAINING AND AUDIT

16.1 We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws.

16.2 We must also regularly test our systems and processes to assess compliance.

16.3 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

16.4 We will regularly review all the systems and processes under our control to ensure they comply with this Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

17. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

17.1 We are required to implement Privacy by Design measures when processing Personal Data. This means implementing appropriate technical and organisational measures to ensure data privacy.

17.2 We must periodically assess what Privacy by Design measures can be implemented on all programs/systems/processes by considering:

- New technologies that are available;
- The cost of implementation;
- The nature, scope, context and purposes of processing;
- The risks to the rights and freedoms of Data Subjects posed by the processing.

17.3 Data controllers must also conduct DPIAs for any high risk processing activities.

17.4 You should conduct a DPIA (and discuss your findings with the DPO) 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 processing of Sensitive Data;
- Large-scale, systematic monitoring of a publicly accessible area.

17.5 A DPIA must include:

(a) a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;
(b) an assessment of the necessity and proportionality of the processing in relation to its purpose;
(c) an assessment of the risk to individuals; and
(d) the risk mitigation measures in place and demonstration of compliance.

18. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

18.1 Automated Decision Making is prohibited when a decision has a legal or similar significant effect on a Data Subject unless:

(a) a Data Subject has given explicit Consented to the processing;
(b) the processing is authorised by law; or
(c) the processing is necessary for the performance of or entering into a contract.

18.2 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed of their right to object. This must happen when we first communicate with them and be communicated clearly and separately from other information.

18.3 We must inform the Data Subject of the logic involved in the decision making or profiling, and its significance and envisaged consequences.

18.4 We must also give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

18.5 A DPIA must be carried out before any Automated Processing (including profiling) or Automated Decision Making activities are undertaken.

19. DIRECT MARKETING

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

19.2 A Data Subject's prior consent is required for electronic direct marketing. However, there is a limited exception for existing customers which allows us to send marketing texts or emails in the following circumstances:

- We have obtained contact details in the course of a sale to that person
- We are marketing similar products or services
- We gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message

19.3 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.

19.4 A Data Subject's objection to direct marketing must be promptly honoured.

19.5 If a Data Subject opts out at any time, their details should be suppressed as soon as possible. Suppression means retaining just enough information to ensure that marketing preferences are respected in the future.

20. SHARING PERSONAL DATA

20.1 We must not share Personal Data with third parties unless certain safeguards (often including contractual arrangements) have been put in place.

20.2 You may only share the Personal Data we hold with other Company Personnel and if the recipient has a job-related need to know the information.

20.3 If sharing the Personal Data involves a cross-border transfer you must ensure you have notified a Responsible Person and have approval to do so.

20.4 You may only share Personal Data we hold with third parties, such as our service providers if:

- They have a need to know the information for the purposes of providing the contracted services
- Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place
- The transfer complies with any applicable cross border transfer restrictions
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

21. CHANGES TO THIS PRIVACY STANDARD

21.1 We may change this Standard to comply with new guidance and best practice. If this happens we will notify all Company Personnel.

22. DEFINITIONS

22.1 Please refer to the following terms which have been used in this Standard.

- **Automated Decision-Making (ADM):** When a decision is made which is based solely on computerised algorithms, or 'Automated Processing' to produce a legal effect or significantly affect an individual, including profiling, credit decisions or matters affecting employment. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

(a) **Automated Processing:** Any form of automated processing of Personal Data, and the evaluation of certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated processing

(b) **Company Personnel:** All employees, workers, contractors, agency workers, volunteers and consultants who are engaged to work for the Company.

(c) **Consent**: The freely-given, unambiguous indication that a Data Subject has provided a positive affirmation that they consent to particular kinds of data being processed for particular purposes. Consent is necessary for certain special categories of sensitive data and in order to justify the processing of data for longer than is required under other legal bases.

(d) **Data Breach:** An act or omission that compromises the security, confidentiality, integrity or availability of Personal Data, or a failing in the technical and organisational safeguards put in place to protect Personal Data. Any unauthorised access, disclosure, loss, damage or destruction qualifies as a Data Breach.

(e) **Data Controller:** An organisation which holds, transfers or otherwise processes Personal Data and is in a position to make a decision about that processing.

(f) **Data Privacy Impact Assessment (DPIA)**: An assessment used to identify and reduce the risks of data processing activities. DPIAs should be undertaken to review any new major systems or activities may involving the processing of Personal Data and identify new risks and how to mitigate them. This can be carried out as part of a Privacy by Design process.

(g) **Data Protection Legislation**: Any applicable law or code of conduct which applies to the processing activities of the Company, which in the UK is the General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (pending at the time this policy was produced).

(h) **EEA:** The European Economic Area, including the 28 countries which make up the EU, and those included in the European Free Trade Agreement: Iceland, Liechtenstein and Norway.

(i) **Data Subject**: A living identifiable individual about whom we hold Personal Data.

(j) **Explicit Consent:** A high level of consent which requires a very clear and specific statement by the Data Subject.

(k) **Personal Data (or 'Data'):** Any information which can identify a natural person either directly or indirectly, alone or in combination with other data. For the purposes of this Policy, the only Personal Data which is captured by the Data Protection Legislation is that which is processed by automated electronic means, or which is organised in any kind of structured filing system which can be searched and individuals found by using specific criteria.

(l) **Privacy by Design:** The process of implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

(m) **Privacy Notice**: Formal written notification given to Data Subjects at the point where their data is collected, outlining which categories of data will be processed, the purpose for processing, retention periods and information about their rights to make requests and complaints.

(n) **processing or process:** Any activity that involves the use of Personal Data, including obtaining, recording, holding or carrying out any operation on the data, such as organising, amending, retrieving, using, disclosing, erasing or destroying it. processing also includes transmitting or transferring Personal Data to third parties.

(o) Pseudonymised Data: Personal Data where any information that directly or indirectly identifies an individual is replaced with one or more artificial identifiers or pseudonyms so that the individual cannot be identified without the use of additional information kept separately an securely.

(p) Responsible Persons: the designated officer or officers within the Company who takes responsibility for matters relating to Data Protection. In our organisation, the Responsible Person is:

Laura Humphrey, Partner, laura@humphreyandbrand.co.uk

(q) Special Categories of Sensitive Data / Sensitive Personal Data: Specific types of protected Sensitive Personal Data, I.E.:

(i) Race or ethnic origin
(ii) Political opinions
(iii) Religious or spiritual beliefs
(iv) Trade union membership
(v) Physical or mental health
(vi) Sexual life and orientation
(vii) Biometric or genetic data

