P.J.KEARY LTD
Jubilee House Townsend Lane London NW9 8TZ
Tel: 020 8202 3090 Fax: 020 8200 8591
Website: www.pjkeary.co.uk

Data Protection Policy

1. Introduction

This Policy sets out the obligations of P J Keary Ltd ("the Company") with regard to data protection and the rights of employees, customers and business contacts ("data subjects") in respect of their personal data under the UK GDPR/Data Protection Act 2018 ("the Act"). Under the Act, "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.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

The Company is registered with the Information Commissioner as a data controller under the register held by the Information Commissioner.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out seven principles with which any party handling personal data must comply. All personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals ('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 not be considered to 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('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')."

Furthermore, it is required that:

g) the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 of the UK GDPR ('accountability').

Personal data must be processed fairly and lawfully, meaning that at least one of the following conditions must be met:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Where the processing special category data (defined below in Part 4 of this Policy), at least one of the following conditions must be met (Article 9):

a) Explicit consent

b) Employment, social security and social protection (if authorised by law)

c) Vital interests

d) Not-for-profit bodies

e) Made public by the data subject

f) Legal claims or judicial acts

g) Reasons of substantial public interest (with a basis in law)

h) Health or social care (with a basis in law)

i) Public health (with a basis in law)

j) Archiving, research and statistics (with a basis in law)

3. Rights of Data Subjects

Under the Act, data subjects have the following rights:

a) the right to be informed about the collection and the use of their personal data

b) the right to access personal data and supplementary information

c) the right to have inaccurate personal data rectified, or completed if it is incomplete

d) the right to erasure (to be forgotten) in certain circumstances

e) the right to restrict processing in certain circumstances

f) the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services

g) the right to object to processing in certain circumstances

h) rights in relation to automated decision making and profiling

i) the right to withdraw consent at any time (where relevant)

j) the right to complain to the Information Commissioner

4. Personal Data

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Act also defines “special category data” as personal data that has a greater ability to harm the individuals if not handled correctly. Special category data is defined as:

a) personal data revealing racial or ethnic origin;

b) personal data revealing political opinions;

c) personal data revealing religious or philosophical beliefs;

d) personal data revealing trade union membership;

e) genetic data;

f) biometric data (where used for identification purposes);

g) data concerning health;

h) data concerning a person's sex life; and

i) data concerning a person's sexual orientation.

The Company only holds personal data that is directly relevant to its dealings with a given data subject. That data will be collected, held, and processed in accordance with the data protection principles and with this Policy.

5. Processing Personal Data

Any and all personal data collected by the Company is collected in order to ensure that the Company can provide the best possible service to its customers, and can work effectively with its partners, associates and affiliates and efficiently manage its employees, contractors, agents and consultants. The Company may also use personal data in meeting certain obligations imposed by law.

Personal data may be disclosed within the Company, provided such disclosure complies with this Policy. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

In particular, the Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully;
- Data subjects are always made fully aware of the reasons for the collection of personal data and are given details of the purpose(s) for which the data will be used;
- Personal data is only collected to the extent that is necessary to fulfil the purpose(s) for which it is required;
- All personal data is accurate at the time of collection and kept accurate and up to date while it is being held and/or processed;
- No personal data is held for any longer than necessary in light of the purpose(s) for which it is required;
- All personal data is held in a safe and secure manner, as detailed in Part 6 of this Policy, taking all appropriate technical and organisational measures to protect the data;
- All personal data is transferred securely, whether it is transmitted electronically or in hard copy;
- No personal data is transferred outside of the European Economic Area (as appropriate) without first ensuring that the destination country offers adequate levels of protection for personal data and the rights of data subjects; and

- All data subjects can fully exercise their rights with ease and without hindrance.

6. Data Protection Procedures

The Company shall ensure that all of its employees, agents, contractors, or other parties working on behalf of the Company comply with the following when working with personal data:

- All emails containing personal data must be encrypted
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient **[**or sent using Royal Mail or a reputable Courier service];
- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from Patrick Keary (Director).
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Patrick Keary (Director);
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- Any unwanted copies of personal data (i.e. printouts or electronic duplicates) that are no longer needed should be disposed of securely. Hardcopies should be shredded and electronic copies should be deleted securely;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise **[**without the formal written approval of Patrick Keary (Director) and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary**]**.

- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Act and approval has been given by the data controller, where the Company are not the data controller;
- All personal data stored electronically should be backed up with backups stored offsite and encrypted;
- All electronic copies of personal data should be stored securely using passwords and data encryption;
- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols **[**All software used by the Company is designed to require such passwords**]**;
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All personal data held by the Company shall be regularly reviewed for accuracy and completeness. If any personal data is found to be out of date or otherwise inaccurate, it should be updated and/or corrected immediately where possible. If any personal data is no longer required by the Company, it should be securely deleted and disposed of;

7. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- The Company has appointed Patrick Keary (Director) as its Data Protection Officer with the specific responsibility of overseeing data protection and ensuring compliance with this Policy and with the Act. The Data Protection Officer shall in particular be responsible for:
    - Overseeing the implementation of, and compliance with this Policy, working in conjunction with the relevant employees, managers and/or department heads, agents, contractors and other parties working on behalf of the Company;
    - Organising suitable and regular data protection training and awareness programmes within the Company;
    - Reviewing this Policy and all related procedures not less than annually;
- All employees, agents, contractors, or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company's responsibilities under the Act and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to and use of personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- The Performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Act;
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

8. Service provision as a data processor

In the course of completing work on behalf of our clients, the Company shall take the role of data processor, with our clients being designated the data controller. In order for the Company to preserve our role as a data processor, it is important that we only processes data in the way defined by our clients.

Our lawful basis for processing the data defined below is to meet the **contractual requirements** placed upon us by our clients. We shall not use data in anyway other than that stated by our clients.

The exact data collected may vary between clients however the following data is typically collected during the course of providing our services:

- For Street Works compliance audits:
  - Name of individual
  - Image of individual's face as part of ID card verification
  - Individual's dates of birth in photographic form if stated on ID cards
  - Individual's professional competencies and membership numbers
- For clarification of Utility supply and billing purposes
  - Customer Names, addresses and contact details (email, phone).

The data will be stored in electronic format in systems employing the security and organisational measures outlined in sections 6 and 7 of this policy. Retention periods shall be defined in line with each client's specific requirements, and wherever feasible, automatic measures will be used to erase data securely at the end if the agreed timeframe.

9. Access by Data Subjects

A data subject may make a subject access request ("SAR") at any time to find out more about the information which the Company holds about them.

- SARs should be made in writing, addressed to Patrick Keary, Director, P J Keary Ltd, Jubilee House, Townsend Lane, London NW9 8TZ .
- A SAR **[**may be made using the Company's Subject Access Request Form, but does not have to be, and if it is not, it**]** should be clearly identifiable as a SAR.
- SARs must make it clear whether it is the data subject themselves that is making the request or whether it is a person acting on his or her behalf. In either case, proof of identity must be provided. If the SAR is made on another's behalf, the individual making the request must provide clear evidence of their authorised capacity to act on behalf of the data subject.
- The Company cannot charge a fee for reasonable SAR

Upon receipt of a SAR the Company shall have a maximum period of one month within which to respond fully **[**but shall always aim to acknowledge receipt of SARs within 10 business days**]**. The following information will be provided to the data subject:

- Whether or not the Company holds any personal data on the data subject;
- A description of any personal data held on the data subject;
- Details of what that personal data is used for;
- Details of how to access that personal data and how to keep it up to date;
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.

10. Notification to the Information Commissioner's Office

As a data controller, the Company is required to notify the Information Commissioner's Office that it is processing personal data. The Company is registered in the register of data controllers, registration number: ZA275761.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

The Data Protection Officer shall be responsible for notifying and updating the Information Commissioner's Office.

11. Implementation of Policy

This Policy has been approved & authorised by:

Name:	Patrick Keary
Position:	Director
Date:	10th October 2023
Due for Review by:	10th October 2024
Signature: