DATA PROTECTION POLICY STATEMENT

I D Corcoran Building Contractors Ltd is committed to protecting the privacy and security of all data held.

This policy describes how we protect data during in accordance with the General Data Protection Regulation (GDPR) and data protection legislation.

The Data Protection Act 2018 protects against the misuse of personal data and may cover both manual and electronic records.

All records held on computer and certain manual files may fall within the Data Protection Act, depending on the ease of access to data within the file. However, for consistency and good practice, the Company will adopt the same approach for all data held.

The Act requires that any data held by the company should be;

- used fairly, lawfully and transparently.
- used for specified explicit purposes.
- used in a way that is adequate, relevant and limited to only what is necessary.
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.
- handled in a way that ensures appropriate security, held securely including protection against unlawful or unauthorised processing, access, loss, destruction or damage.
- not transferred to a country outside the European Economic Area unless there is an adequate level of data protection in that country.

Our process/procedures;

- ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law.
- not do anything with the data held that the individual would not expect given the content of this policy and the privacy notice.
- ensure that appropriate privacy notices are in place advising staff and others how and why their data is being processed, and, in particular, advising data subjects of their rights.
- only collect and process the sensitive data that is needed for purposes it has identified in advance.
- ensure that, as far as possible, the data held is accurate, or a system is in place for ensuring that it is kept up to date.
- only hold onto data for as long as needed, after which time it will be securely erased or destroyed.
- ensure that appropriate security measures are in place so that personal data can only be accessed by those who need to access it and that it is held and transferred securely.

Who has access to data held within the company:

We may share information with third parties where required by law, where it is necessary or where we have another legitimate interest in doing so.

Recipients of data may include third-party service providers (other members of staff within the company), other related business entities, a regulator or to otherwise comply with the law.

Where we do so, we will require third parties to respect the security of data and to treat it in accordance with the law.

We may transfer personal information outside the EU. If we do, it is to be expected a similar degree of protection is in place in respect of this information.

All members of staff are responsible for ensuring that any data which they hold is kept securely and not disclosed to any unauthorised third parties. We will ensure that all information is accessible only to those who have a valid reason for using it.

Security of data:

We have put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal information to those employees, agents, contractors and other third parties who have a business need to know.

We have put in place procedures to deal with any suspected data security breach and will notify the individual and any applicable regulator of a suspected breach where we are legally required to do so.

We have in place appropriate security measures including:

- Keep all sensitive data in a lockable cabinet with key controlled access.
- Password protect personal/sensitive data held electronically.
- Archive data which is then kept securely.
- Ensure that PC screens are not left unattended without password protected screensaver being used so data is only visible to authorised members of staff.
- Ensure all visitors are accompanied whilst on the premises.
- Any individuals who need access to view various documentation containing sensitive data (e.g. external IT support, auditors etc.) are to sign the 'Data Access Memo' that is currently in place to protect any sensitive information held in agreement of the conditions stated within it.

In addition, we will put in place appropriate measures for the deletion of data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or, if that is not possible, destroyed physically. This policy also applies to members of staff who process sensitive data 'off-site' e.g. when working at home, and in these circumstances additional care must be taken regarding the security of all data.

How we decide how long to retain data:

We hold a variety of data from all clients, employees, suppliers and sub-contractors new and old. We will only retain information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for data we consider the amount, nature, and sensitivity of the data as well as the potential risk of harm from unauthorised use or disclosure of

data, the purposes for which we process data, whether we can achieve those purposes through other means and the applicable legal requirements.

I D Corcoran Building Contractors Ltd reviews the need to remove data accordingly, whether it has been requested by the individual or it is no longer needed.

Changes to the privacy policy:

I D Corcoran Building Contractors Ltd reserves the right to update this privacy notice at any time and we will provide a new privacy notice when we make any substantial updates. This policy will be reviewed annually from the date of the last review and/or change (whichever is the latest) to ensure its continuing relevance and accuracy. We may also notify in other ways from time to time regarding the processing information.

The Data Protection Act 1998 protects employees against the misuse of personal data and may cover both manual and electronic records.

All records held on computer fall within the Data Protection Act. Certain manual files may also fall within the Act, depending on the ease of access to data within the file. However, for consistency and good practice, I D Corcoran Building Contractors Ltd will adopt the same approach for data held.

The Act requires that any personal data held should be:

- Processed fairly and lawfully;
- Obtained and processed only for specified and lawful purposes;
- Adequate, relevant and not excessive;
- Accurate and kept up to date;
- Held securely and for no longer than is necessary; and
- Not transferred to a country outside the European Economic Area unless there is an adequate level of data protection in that country.

The Act also gives employees certain rights. For employment purposes, the most important right is the right to access the personal data held about the employee.

Purposes for which Personal Data may be Held

Personal data relating to employees may be collected primarily for the purposes of:

- Recruitment, promotion, training, redeployment and/or career development;
- Administration and payment of wages;
- Calculation of certain benefits including pensions;
- Disciplinary or performance management purposes;
- Performance review;
- Recording of communication with employees and their representatives
- To record digital meetings to allow replay or storage:
- Compliance with legislation;
- Provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and
- Staffing levels and career planning.

The Company considers that the following personal data falls within the categories set out above:

- Personal details including name, address, age, status and qualifications.
  Where specific monitoring system are in place, ethnic origin and nationality will also be deemed as relevant;
- References and CVs;
- Emergency contact details;
- Notes on discussion between management and the employee;
- Appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment;
- Training records;
- Salary, benefits and bank/building society details; and
- Absence and sickness information.

Employees or potential employees will be advised by the Company of the personal data which has been obtained or retained, its source, and the purpose for which the personal data may be used or to whom it will be disclosed.

The Company will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for a requiring the information to be retained

Sensitive Personal Data

Sensitive personal data includes information relating to the following matters:

- The employee's racial or ethnic origins;
- His or her political opinions;
- His or her religious or similar beliefs;
- His or her trade union membership;
- His or her physical or mental health or condition;
- His or her sex life; or
- The commission or alleged commission of any offence by the employee.

To hold sensitive personal data, the Company must additionally satisfy a sensitive data condition. The most appropriate condition for employment purposes is that the processing is necessary to enable the Company to meet its legal obligations (for example, to ensure health and safety or to avoid unlawful discrimination).

Responsibility for the Processing of Personal Data

The Company will appoint a Data Controller as the named individual responsible for ensuring all personal data in controlled in compliance with the Data Protection Act 1998.

Employees who have access to personal data must comply with this Policy and adhere to the procedures laid down by the Data Controller. Failure to comply with this Policy and procedures may result in disciplinary action up to and including summary dismissal.

Use of Personal Data

To ensure compliance with the Data Protection Act 1998 and in the interests of privacy, employee confidence and good employee relations, the disclosure and use of information held by the Company is governed by the following conditions:

- Personal data must only be used for one or more of the purposes specified in this Policy;
- Company documents may only be used in accordance with the statement within each document stating its intended use;
- Provided that the identification of individual employees is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data (e.g. surveys, staffing level figures); and
- Personal data must not be disclosed, either within or outside the Company, to any unauthorised recipient.

Personal Data Held for Equal Opportunities Monitoring Purposes

Where personal data obtained about candidates is to be held for the purpose of equal opportunities monitoring, all such data must be made anonymous.

Disclosure of Personal Data

Personal data may only be disclosed outside the Company with the employee's written consent, where disclosure is required by law or where there is immediate danger to the employee's health.

Accuracy of Personal Data

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date.

In order the ensure the Company's files are accurate and up to date, and so that the Company is able contact the employee or, in the case of an emergency another designated person, employees must notify the Company as soon as possible of any change in their personal details (e.g., change of name, address; telephone number; loss of driving licence where relevant; next of kin details, etc.).

Standard printouts of personal records will be issued to all employees on an annual basis for the purposes of ensuring the data is up to date and accurate. Employees will be entitled to amend any incorrect details and these corrections will be made to all files held on the Company's information systems. In some cases, documentary evidence e.g., qualification certificates, will be requested before any changes are made.

Once completed, these records will be stored in the employee's personnel file.

Access to Personal Data ("Subject Access Requests")

Employees have the right to access personal data held about them. The Company will arrange for the employee to see or hear all personal data held about them within 40 days of receipt of a written request and subject to a £10.00 administration fee.

Signature: 

Name: Mr D A Corcoran

Position: Managing Director

Date: 25th May 2023

Review Date: 25th May 2024