JFA Environmental Planning

BRINGING NATURE TO THE HEART OF DESIGN

DATA PROTECTION POLICY

Introduction

JFA is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act") and the General Data Protection Regulation (GDPR) which comes into effect on 25th May 2018. The Company will therefore follow procedures that aim to ensure that all employees, sub-contractors, agents, consultants, partners or other servants of the Company who have access to any personal data held by or on behalf of the Company, are fully aware of and abide by their duties and responsibilities under the Act and GDPR.

Statement of policy

In order to operate efficiently, JFA Environmental Planning has to collect and use information about people with whom it works. These may include past and prospective employees, clients and suppliers. The only personal data JFA holds relating to our clients are business related: names, titles, business addresses and business emails. We collect similar basic business information for anyone who signs up for the newsletter. Data is collected is held on employees. All daa is handled and dealt with properly, and whether it be on paper, in computer records or recorded by any other means, following the safeguards set out within the Act and GDPR to ensure this.

JFA Environmental Planning regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Company and those with whom it carries out business. The Company treats the limited personal information it holds lawfully and correctly.

To this end the Company fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998 and under the GDPR guidelines.

The Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with principles of good practice. Those relevant principles are legally enforceable.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **"sensitive" personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- Data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes an 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.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;

- Trade Union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

JFA holds no sensitive personal data on any employee, customer or supplier.

General Data Protection Regulation

Alongside the stipulations of the Data Protection Act 1998, GDPR states that data may not be processed unless there is at least one lawful basis to do so. Those relevant to JFA are:

- The data subject has given consent to the processing of personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.

Handling of personal/sensitive information

JFA Environmental Planning will, through appropriate management and the use of strict criteria and controls:

- Fully observe conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which the information is used;
- Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act and GDPR.

  These include:
  - The right to be informed that processing is being undertaken;
  - The right of access to one's personal information within the statutory 40 days;
  - The right to prevent processing in certain circumstances;
  - The right to correct, rectify, block or erase information regarded as wrong information.

In addition, the Company will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a third party, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All JFA Environmental Planning staff are fully aware of this policy and of their duties and responsibilities under the Act and GDPR.

All Managers and staff within the Company will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All sub-contractors, consultants, partners or other servants or agents of the Company must:

- Ensure that they, and all of their staff who have access to personal data held or processed for or on behalf of the Company, are aware of this policy and are fully trained and are aware of their duties and responsibilities under the Act and GDPR. Any breach of any provision of the Act or GDPR will be deemed as being a breach of any contract between the Company and that individual, company, partner or firm;
- Allow data protection audits by the Company of data held on its behalf (if requested);
- Indemnify the Company against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All sub-contractors who are users of personal information supplied by the Company will be required to confirm that they will abide by the requirements of the Act and GDPR with regard to information supplied by the Company.

_____

This Policy Was Last Updated 24th May 2018