General Data Protection Regulation (GDPR) Policy

Introduction

John Turner Construction Group (the Company) needs to collect and use certain types of information about its employees and others with whom it comes into contact in order to operate as a business. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database or recorded on other material and there are safeguards to ensure this under the General Data Protection Regulation 2016 (GDPR).

Policy statement

The Company intends to ensure that personal information is treated lawfully and correctly. To this end the Company endorses fully and adheres to the six principles of data protection, as set out in the Article 5 of the GDPR:

- data will be processed lawfully, fairly and in a transparent manner in relation to individuals
- data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- data will be 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
- data will be 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
- data will be 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.

These principles will be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the Company will:

- observe fully the conditions regarding the fair collection and use of information, including the giving of consent
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (ie the right to be informed that processing is being undertaken, to access one’s personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- take appropriate technical and organisational security measures to safeguard personal information
- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection
- ensure that personal information is not transferred abroad without suitable safeguards.

The Company will ensure that the rights of those about whom information is held, can be fully exercised under the Act. These include:

- the right to be informed that processing is being undertaken

- the right of access to one's personal information
- the right to prevent processing in certain circumstances and
- the right to correct, rectify, block or erase information which is regarded as wrong information
- the right to be forgotten.

Data Controller

Under the GDPR the Data Controller post is held by the Company's Finance Director. This role determines for what purpose any personal information held will be used. This role is also responsible for notifying the Information Commissioner's Office of the data it holds or is likely to hold and the general purposes that this data will be used for.

Data Protection Officer

Under the GDPR the Data Protection Officer for all employee related data is the Company's HR Manager. The Data Protection Officer for all other categories of personal data outside of employee data, such as those relating to subcontractors, suppliers and other third parties is the Company's Facilities Manager.

Data Subject

Under the GDPR a "Data Subject" is any individual who can be identified or distinguished from another from personal data held, e.g. an employee. Data Subjects have certain rights:

- the Data Controller must provide Data Subjects with information about the Company's processing activities
- Data Subjects have the right to request access to their data which is being processed by a Data Controller
- Data Subjects have the right to get incorrect information corrected by the Data Controller, and/or complete incomplete information. The Data Controller is also obliged to notify any third party processors of the request for rectification, for example pension providers or the HMRC
- Data Subjects may object to their information being held and used
- Data Subjects have the right to have their personal information erased by making a request to the Data Controller
- Data Subjects will have the right to be provided with their data in a structured, commonly used electronic format
- Data Subjects can exercise the right to restrict processing of data in certain circumstances. In these cases, apart from storing "static" data, information can only be processed (or used) either: with the Data Subject's consent; in connection with legal claims; to protect the rights of another person; or if it is for reasons of important public interest.

Data collection

Informed consent is when:

- a Data Subject understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- and then gives their consent.

The Company will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person or by completing a form.

When collecting data, the Company will ensure that the Data Subject:

- understands why the information is needed
- understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing

- as far as reasonably possible, grants explicit written consent for data to be processed
- is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.

Data storage

Information and records relating to Data Subjects will be stored securely and will only be accessible to authorised individuals.

Information will be stored for only as long as it is needed or required by law and will be disposed of appropriately.

It is the Company's responsibility to ensure all personal and Company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Data access and accuracy

All Data Subjects have the right to access the information the Company holds about them. The Company will also take reasonable steps to ensure that this information is kept up to date by periodically asking Data Subjects whether there have been any changes. In addition, the Company will ensure that:

- everyone processing personal information understands that they are contractually responsible for following good data protection practice
- everyone processing personal information is appropriately trained to do so
- everyone processing personal information is appropriately supervised
- anybody wanting to make enquiries about handling personal information knows what to do
- it deals promptly and courteously with any enquiries about handling personal information
- it describes clearly how it handles personal information
- it will regularly review and audit the ways it holds, manages and uses personal information
- it regularly assesses and evaluates its methods and performance in relation to handling personal information
- all employees are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken.

Disclosure

The Company may share data with other organisations when it is appropriate to do so, for example HMRC or the DVLA.

Data Subjects will be made aware in most circumstances how and with whom their information will be shared. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties, for example childcare vouchers or healthcare
- disabled employees - whether any reasonable adjustments are required to assist them at work
- employee's health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management of occupational health - to consider how an employee's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

There are circumstances where the law allows the Company to disclose data (including sensitive data) without the Data Subject's consent. These are:

- carrying out a legal duty or as authorised by the Secretary of State

- protecting vital interests of an employee or other person
- the employee or other person has already made the information public
- conducting any legal proceedings, obtaining legal advice or defending any legal rights
- monitoring for equality and diversity purposes e.g. race, disability or religious belief.

The right to be forgotten

The Company recognises the inherent right for an individual to be forgotten. This means that on request for the individual all information held is securely destroyed and proof given of such destruction. In certain circumstances (for example legal defence) the Company may refuse in part or in full to comply with the request.

Disaster recovery

The Company backs up data every day and has multiple copies (at least one set for each day of the week and additional weekly ones in order to have at least a month's worth of data at any one time). Records of these are kept:

- backups are kept off-site or in special heat-proof safes
- backups are verified regularly by the software and system supplier
- master copies of software are stored off site or in a heat-proof safe
- firewalls and virus checkers are kept up to date and running, and users are trained in virus avoidance and detection
- computers are protected from physical harm, theft or damage, and from electrical surges using protective plugs
- the Company plans for how to deal with loss of electricity, external data links, server failure, and network problems. It uses paper forms where necessary for temporary record keeping.

Policy review and amendment

This policy is subject to review and amendment in line with prevailing legislation and best practice. The Company reserves the right to review and amend this policy at any time.

Signed:

John Clarke

Managing Director

Issued: May 2018 and reviewed annually thereafter

Latest review: January 2022