

EE Civil Engineering is committed to the importance of complying with data protection legislation as covered by the Data Protection Act 2018, and dictated under General Data Protection Regulation. Data Protection Legislation regulates the capture, storage and use of information about individuals, known as "personal data".

Introduction

The principles under the Data Protection Act require that personal data, including that of our employees and third parties are:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

EE Civil Engineering Ltd are registered with the Information Commissioner to process personal data. EE Civil Engineering are named as a data controller under the register kept by the Information Commissioner in accordance with the Data Protection Act.

During the course of an individual's employment, they may come into contact with and use confidential personal information about other employees, clients, customers, suppliers, providers, agents, contractors and other people, such as their names, email addresses and home addresses.

This policy helps them to ensure that they do not breach the Data Protection Act 2018. There are strict rules governing the collection, retention, storage, use and disclosure of personal information.

It is a criminal offence to disclose personal data knowingly or recklessly in breach of the Data Protection Act 2018 and any such action could also result in significant fines for the Company, as well as irreparable damage to the Company's reputation.

The Company is a "Data Controller". This means that we are responsible for deciding how we hold and use personal information.

1.0 Information we hold

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We may collect, store, and use the following categories of personal information.

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependents.

- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving license.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process); Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about the use of our information and communications systems.
- Photographs.

We may also collect, store, and use the following "special categories" of more sensitive personal information.

- Information about race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Information about health, including any medical condition, health, and sickness records.
- Information about criminal convictions and offences.

2.0 How personal information is collected

We typically collect personal information about employees, workers and contractors through the application, recruitment, and induction process, either directly from candidates or sometimes from an employment agency or background check provider.

We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies i.e. Disclosure Barring Services. We will collect additional personal information during job-related activities throughout the period of you working for us.

Human Resources will conduct an annual data accuracy review with employees to ensure the data we hold is accurate and up to date.

3.0 How we use personal information

We will only use personal information when the law allows us to. Most commonly, we will use personal information in the following circumstances:

- Where we need to perform the contract, we have entered into with an individual
- Where we need to comply with a legal obligation
- Where it is necessary for our legitimate interests (or those of a third party) and an individual's interests and fundamental rights do not override those interests.

We may also use personal information in the following situations, which are likely to be rare:

- Where we need to protect an individual's interests (or someone else's interests)
- Where it is needed in the public interest (or for official purposes).

4.0 Situations in which personal information is used

We need all the categories of information in the list above (see section 2.0) primarily to allow us to perform our contract with an individual and to enable us to comply with legal obligations. In some cases, we may use personal information to pursue legitimate interests of our own or those of third parties, provided an individual's interests and fundamental rights do not override those interests. The situations in which we may process your personal information are listed below, and this list is not exhaustive.

- Making a decision about recruitment or appointment.
- Determining the terms on which an individual work for us.
- Checking an individual is legally entitled to work in the UK.
- Making payments, if they are an employee, deducting tax and National Insurance contributions.
- Enrolment into the Company's benefit schemes i.e. Pension, Private Medical Insurance, Salary Sacrifice Extras, Occupational Health, ECIS benefits; Liaising with the dedicated pension provider.
- Administering the contract, we have entered into.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance & determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving an individual, or other employees, workers and contractors, including accidents at work.
- Ascertaining fitness to work.
- Managing sickness absence.
- Complying with Health & Safety obligations.
- To determine whether we need to make reasonable adjustments to the workplace or role because of a disability.
- To answer questions from insurers in respect of any insurance policies.
- To comply with employment law, immigration law, health and safety law, tax law and other laws which affect us.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- For any other reason which we may notify an individual of from time to time.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of personal information.

Personal data that we hold (whether sensitive or otherwise), will only contain the minimum amount of data that we require to comply with our obligations, and it will only be retained for as long as it is required to enable us to comply with our legal obligations. After this time, it will be permanently deleted. All data is retained in accordance with our Data Retention Policy, a copy of which is available on IMS.

5.0 Failing to provide personal information

If an individual fails to provide certain information when requested, we may not be able to perform the contract we have entered into with them (such as paying them or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the Health & Safety of our workers).

6.0 Change of purpose

We will only use personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so. Please note that we may process personal information without knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

7.0 How sensitive personal information is used

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing, and using this type of personal information. We may process special categories of personal information in the following circumstances.

- In limited circumstances, with an individuals' explicit written consent.
- Where we need to carry out our legal obligations.
- Where it is needed in the public interest, such as for equal opportunities monitoring, or in relation to our occupational pension scheme.
- Where it is needed to assess an individuals' working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect an individual's interests (or someone else's interests) and they are not capable of giving their consent, or where they have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

8.0 Our obligations as an Employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws
- We will use information about physical or mental health, or disability status, to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits
- We will use information about race or national or ethnic origin, religious, philosophical, or moral

beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

9.0 Do we need your consent?

We do not need consent if we use special categories of personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law.

In limited circumstances, we may approach an individual for written consent to allow us to process certain particularly sensitive data. If we do so, we will provide them with full details of the information that we would like and the reason we need it, so that they can carefully consider whether they **wish** to consent. Individuals should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

10.0 Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our policies. Less commonly, we may use information relating to criminal convictions where **it** is necessary in relation to legal claims, where it is necessary to protect an individual's interests (or someone else's interests) and they are not capable of giving consent, or where they have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by an individual in the course of them working for us.

Data sharing

We may have to share data with third parties, including third-party service providers and other entities in the group. We require third parties to respect the security of data and to treat it in accordance with the law. We may transfer your personal information outside the EU. If we do, an individual can expect a similar degree of protection in respect of your personal information.

Why might we share personal information with third parties?

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

Which third-party service providers process personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers.

- Payroll
- Accountants
- Pension administration
- Benefits provision and administration

- IT services
- Training providers

How secure is information with third-party service providers & other entities?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect personal information in line with our policies. We do not allow our third-party service providers to use personal data for their own purposes. We only permit them to process personal data for specified purposes and in accordance with our instructions.

When might we share personal information with other entities in the group?

We will share personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

12.0 Data Security & Breaches

We have put in place measures to protect the security of an individuals' information. Details of these measures are contained with the relevant policies that are available on IMS. Third parties will only process personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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. They will only process personal information on our instructions, and they are subject to a duty of confidentiality.

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of an individual or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office (ICO) within 72 hours. If any individual is aware of a data breach, they must contact the Company's Head of IT immediately and keep any evidence they have in relation to the breach.

13.0 Data Retention

We will only retain personal 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. Details of retention periods for different aspects of your personal information are available in the relevant policy which is available on IMS.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

14.0 Rights of Access, Correction, Erasure, and Restriction

It is important that the personal information we hold is accurate and current. Individuals must keep us informed if their personal information changes during their working relationship with us. Under certain circumstances, by law they have the right to.

- **Request Access** to personal information (commonly known as a "data subject access request"). This enables them to receive a copy of the personal information we hold about them and to check that we are lawfully processing it.
- **Request Correction** of the personal information that we hold about them. This enables them to have any incomplete or inaccurate information we hold corrected.
- **Request Erasure** of personal information. This enables them to ask us to delete or remove personal information where there is no good reason for us continuing to process it. They also have the right to ask us to delete or remove your personal information where they have exercised the right to object to processing (see below).
- **Object to Processing** of personal information where we are relying on a legitimate interest (or those of a third party) and there is something about a particular situation which makes them want to object to processing on this ground. They also have the right to object where we are processing their personal information for direct marketing purposes.
- **Request the Restriction** of processing of personal information. This enables them to ask us to suspend the processing of personal information about them, for example if they want us to establish its accuracy or the reason for processing it.
- **Request the Transfer** of personal information to another party.

If you want to review, verify, correct, or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact Human Resources in writing. You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

15.0 Right to withdraw consent

In the limited circumstances where an individual may have provided their consent to the collection, processing, and transfer of personal information for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. To withdraw consent, please contact Human Resources.

Once we have received notification that they have withdrawn their consent, we will no longer process their information for the purpose or purposes they originally agreed to, unless we have another legitimate basis for doing so in law.

16.0 Changes to this Data Protection Policy

We reserve the right to update this policy at any time, and an updated policy will be available on SharePoint. We may also notify you in other ways from time to time about the processing of personal information.

If you have any questions about this Data Protection Policy, please contact the Managing Director.

Signed:



Name: Ryan Doherty

Position: Managing Director

Issue Date: 01/06/2026

Review Date: 01/06/2027