General Data Protection Regulations (GDPR) Policy

Policy Information	
Organisation	J. Coffey Construction Ltd and the Company's associated Divisions namely, Main Contract Division, Infrastructure Division and the Plant Division forming the Organisation and those so named who deal with relevant Personal Data for and on behalf of the Organisation, will have reviewed the appropriate lawful basis for each activity of data gathering and are therefore responsible as the 'Data Controller' in determining the purpose for which and the manner in which any personal data are to be processed.
Scope of the Policy	The scope of the policy will apply to all parts of the organisation previously named with regards to the personal details required for the purposes of employment or engagement. Data processing will be predominantly in house, but external parties who are party to some elements of data as previously named acting on our behalf will be the following: • Daines Kapp Insurers • The Workers Guild • Medigold (Occupational Health) • CITB
Policy Operational Date	This policy will commence operationally from May 25th 2018
Policy Prepared By	AC as IMS Systems Director with ongoing responsibility to be appointed in due course. With regards to any sensitive data being processed a Data Protection Officer DPO will be duly appointed if employees for the company exceed two hundred and forty nine and who will then review and prepare a relevant policy to ensure it is compliant to the GDPR requirements
Date Approved by Board	The Board of Directors of the organisation have reviewed the content of this policy and have approved its implementation as of 21st May 2018
Policy Review Date	The Board of Directors of the organisation have reviewed the content of this policy and have approved its implementation as of 21st May 2018

Introduction	
Purpose of the Policy	The purpose of this policy is for the following but not limited to: • be appropriate to the purpose of the Organisation • provide a framework for setting PIMS objectives • be available as documented information • be communicated within the organisation • complying with the law • following good practice • protecting clients, staff and other individuals • be available to interested parties as appropriate • protecting the organisation

	The Organisation is committed to satisfy all applicable requirements of this policy along with a commitment to continually improve this data protection policy. The Organisation further commits to compliance with data protection requirements and good practice including: • processing personal information only where this is strictly necessary and regulatory purposes, or for legitimate organizational purposes. • processing only the minimum personal information required for these purposes. • providing clear information to natural persons (including children) about how their personal information can be used and by whom. • only processing relevant and adequate personal information • processing personal information fairly and lawfully. • maintaining a documented inventory of the categories of personal information processed by the organization. • keeping personal information accurate and, where necessary, up-to-date. • retaining personal information only for as long as is necessary for legal or regulatory reasons or for legitimate organizational purposes and ensuring timely and appropriate disposal. • respecting natural persons' rights in relation to their personal information. • keeping all personal information secure • only transferring personal information outside the UK in circumstances where it can be adequately protected. • the application of the various exemptions allowable by data protection legislation. • developing and implementing a PIMS to enable the PIMS policy to be implemented • where appropriate, identifying internal and external interested parties and the degree to which they are involved in the governance of the organization's PIMS • the identification of workers with specific responsibility and accountability for the PIMS • maintain records of processing of personal information
Type of Data	Types of data stored and controlled will include those previously named in the Scope of the policy and also data such as: • Name, address, and other contact details • Date of birth • CVs, application forms, interview notes, test results, education and training records. • Employment contract(s) and amendments to the same. • Appraisals and performance information. • Records (accident, sickness, attendance). • References. • Passport & Driving Licence information. • Medical information. • Next of kin contact details. • Immigration / right to work information. • Trade Union membership. • Ethnic/racial origin. • Images (e.g. ID cards, photos, CCTV) • Accident investigation

	• Health & Safety incidents • Vehicle collisions • Inadvertent incidents involving members of the public https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
Policy Statement	J. Coffey Construction Ltd. has a commitment to: • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently • If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will inform those individuals without undue delay. • Notify the Information Commissioner voluntarily, even if this is not required The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The organisation will do this within 72 hours of becoming aware of the breach. • The Organisation ensures to have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals. • Records of any personal data breaches, regardless of whether you are required we are required to notify will be retained. (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)
Key Risks	The key risks within your organisation are in three main areas: • information about data getting into the wrong hands, through poor security or inappropriate disclosure of information that might cause distress to the natural persons if the information is compromised • individuals being harmed through data being inaccurate or insufficient • risk of operational and reputational damage to the organisation

Responsibilities	
The Board / Company Directors	The Board/Company Directors, have overall responsibility for ensuring that the organisation complies with GDPR and other legal obligations.
Data Protection Officer	The responsibilities of the DPO shall include but not limited to: • Briefing the Board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data

	• Approving contracts with Data Processors The Data Protection Officer will be appointed on their professional qualities and expert knowledge on data protection law and practices. This can be a staff member or an external service provider. Either way, we will provide contact details to the relevant data protection authorities. The company will ensure the data protection office is given all appropriate resources to carry out their tasks and maintain their expert knowledge. The Data Protection Officer reports directly to the highest level of management and must not carry out any other tasks that could result in a conflict of interest.
Specific Department Heads	Specific Department heads with access to personal data are: • Head of Health & Safety (Data associated to Accident investigation & Training) • Human Resource/Payroll (Data associated to eligibility to work in the UK, Next of Kin) • Managing Surveyor (Data associated to timesheets and approved payments)
Employees & Volunteers	All staff and volunteers should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)
Enforcement	Part of any training provided will advise employees what penalties can be applied for infringing data protection and related policies, also advise of training that can be provided and the methods of reporting internally

Security	
Scope	Data Security is not wholly a Data Protection issue. Business Continuity is a fundamental part of data protection. Refer to The Business Continuity plan in Attachment 32.1 on the K drive
Setting Security Levels	The greater the consequences of a breach of confidentiality, the tighter the security should be, to that end we will provide support training that includes: • An initial introduction to IT security, covering the risks, basic security measures, company policies and where to get help • Training on how to use company systems and security software properly • On request, a security health check will be carried out on their computer, tablet or phone. In the event of a breach of confidentiality, the Organisation shall notify the national supervisory authority of data breaches which put natural persons at risk within 72 hours and to individuals as soon as possible. Where appropriate, the Organisation shall communicate to the individual all breaches of high risk personal information so that the individual can take appropriate measures.
Security Measures	Security measures implemented to ensure secure data protection includes the following: • Laptop and desktop anti-malware • Server anti-malware

	• Cloud-hosted email spam, malware and content filtering • Email archiving and continuity • Website malware and vulnerability scanning • Intrusion detection and prevention • Desktop firewall • Perimeter firewall It is also your responsibility of the user to use their devices (computer, phone, tablet etc.) in a secure way. However, we will provide training and support to enable you to do so (see below). At a minimum: • Remove software that you do not use or need from your computer • Update your operating system and applications regularly • Keep your computer firewall switched on • For Windows users, make sure you install anti-malware software (or use the built-in Windows Defender) and keep it up to date. For Mac users, consider getting anti-malware software. • Store files in official company storage locations so that it is backed up properly and available in an emergency. • Switch on whole disk encryption • Understand their privacy and security settings on their phone and social media accounts and • Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work computer separate from any family or shared computers. • Don't use an administrator account on your computer for everyday use • Make sure your computer and phone logs out automatically after 15 minutes and requires a password to log back in. When people leave a project or leave the company, we will promptly revoke their access privileges to company systems.
Business Continuity	The Business Continuity Plan is located in attachment 32.1 on the company K drive advising backup procedures (both for data and for key employee availability) and emergency planning.
Specific Risks	As with any company and their operation, a number of risks can arise from a number of areas such as, unknown email contacts, cold calling, informal chats in social circumstances and addressing "vishing" and "phishing" where employees are tricked into giving away information over the phone or by email. It should be noted that special precautions should be taken when information is in particularly risky situations, such as being worked on at home, with clients, at meetings, etc. Care should be taken and employees vigilant with regards to providing contact details over the phone.

Data Recording and Storage	
Accuracy	Data accuracy is paramount where information is taken over the telephone, how it is checked and confirmed back to the individual? If information is supplied by a third party, what steps will be taken to ensure or check its accuracy? Training provided to relevant personnel should include controls advising best practice to ensure utmost accuracy when taking details of individuals

Updating	Retained Data should be checked during a regular cycle to see if it is required to be maintained or if it can be deleted in a compliant controlled manner, noting the different requirements for different types of data. It should be further noted that CVs cannot be kept for longer than 6 months unless you have express permission from the candidates.
Storage	Refer to the GDPR excel spreadsheet mapping tool and company archiving procedures
Retention periods	Retention periods for different types of data records are recorded in the 30.1 IMS manual on page 21, though these are not retention periods for personal data which will be based on a case by case basis. It should be noted that the current IMS manual is under review to revise in accordance to the new ISO 45001 H&S standard which the organisation is in the process of transition prior to being audited for certification
Archiving	As previously advised
Secure Disposal	All confidential documentation will be securely disposed taking into account the following criteria: • Retention Periods • Updating • Removal of consent Disposal is first as approved by DPO and /or Department Heads

Right of Access	
Responsibility	Any request for right of access should be handled by the appropriate department head and handled within the legal time limit which is one month
Procedure for Making Request	Right of access requests must be in writing and issued on the appropriate 'Right of Access' request form. There should be a clear responsibility on all employees to pass on anything which might be a subject access request to the appropriate person without delay. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
Provision for Verifying Identity	Where the person managing the access procedure does not know the individual personally there should be provision for checking their identity before handing over any information
Charging	Information requested will be provided free of charge. However a 'reasonable fee' can be requested when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also reserve the right to charge a reasonable fee to comply with requests for further copies of the same information. Though this does not mean that the Organisation can charge for all subsequent access requests. The fee will be based on the administrative cost of providing the information
Procedure for Granting Access	If the request is made electronically, we will provide the information in a commonly used electronic format. The GDPR includes a best practice recommendation that, where possible,

	organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.

Transparency	
Commitment	The organisation shall explain its commitment to ensuring that Data Subjects are aware that their data is being processed and • for what purpose it is being processed • what types of disclosure are likely • how to exercise their rights in relation to the data
Procedure	There will be standard ways for each type of Data Subject to be informed, these could be given, for example: • the handbook for employees • in the welcome letter or pack for members, with occasional reminders in the newsletter • during the initial interview with clients • on the web site •
Responsibility	Different teams or employees will be responsible for transparency in relation to different types of Data Subject and the type of data kept, along with the varying control measures associated. Each member with such responsibilities will have been duly and comprehensively versed on their responsibility and commitment to ensure no breach of compliance to the GDPR

Lawful Basis	
Underlying Principles	GDPR states you must record the lawful basis for the personal data you hold and you should set your basis for each Data Subject type here (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/)
Opting out	Even where the organisation is not relying on consent, it may wish to give people the opportunity to opt out of their data being used in particular ways
Withdrawing consent	The organisation may wish to acknowledge that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn

Employee Training & Acceptance of Responsibilities	
Induction	All employees who have access to any kind of personal data shall have their responsibilities outlined during their induction, which will advise them about all relevant control procedures along with the contents of this policy. Attendees to the induction will sign a briefing register confirming they understood their responsibilities

Continuing Training	Any opportunities to raise Data Protection issues during employee induction, training, team meetings, supervisions will be duly considered so as to enhance controls at an administrative level to ensure greater safeguarding of data information
Procedure for Staff Signifying Acceptance of Policy	Conveyance of the data policy will form part of any Employee induction which will provide the opportunity to clarify any queries, so all will understand their responsibilities and sign off their acceptance of that which is stated

Policy Review	
Responsibility	Review of the Policy status will be subject to the in house committee consisting of relevant department heads and the approval of the board of directors after relevant recommendations have been made and applied to the current policy
Procedure	The policy review procedure will consist of the following; • Review of any internal auditing carried out on the policy with regards to compliance to GDPR • Review any non-conformances and actions taken to address • Review of any potential breach and relevant actions taken to address • Review of any change of legislation and requirements to revise the policy • Apply any relevant changes to the policy as found by the review • Issue to the board for formal review and approval prior to sign off •
Timing	Review to be held annually

For more information, please visit the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

When using a third party data processor, please read the guidelines here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Directors Commitment

We, the Directors, pledge to provide satisfactory resources to ensure, so far as reasonably practicable, that our company employees are provided with the necessary training, supervision, information, procedures, skills, equipment and leadership necessary to achieve our Data Policy objectives.

This policy applies to all employees and other personnel engaged in J Coffey Construction operations:

Date: 01.05.19

Signed:

James Coffey
Managing Director

On behalf of J. Coffey Construction