Data Protection (Privacy) Policy

1.0 Introduction

The Data Protection Act 1998 and the General Data Protection Regulations requires every data controller who is processing personal data to notify the appropriate person or organisation unless they are exempt. Failure to notify is a criminal offence. Total Aggregates Ltd will hold and treat the following data in compliance with GDPR:

- Staff administration
- Advertising, marketing and public relations.
- Accounts and records
- Administration of training and training records
- Assessing competencies of suppliers and subcontractors (where used).
- Internal accident/incident investigation and analysis
- CCTV footage of office and yard, and in-vehicle cameras

If any of the above changes, or we need to collect data for any purpose not stated above, we will notify the Information Commissioners Office (ICO) before collecting that data.

2.0 Eight Data Protection Principles

Whenever collecting information about people, the company is committed to applying the Eight Data Protection Principles:

1. Personal data should be processed fairly and lawfully
2. Personal data should be obtained only for the purpose specified
3. Data should be adequate, relevant and not excessive for the purposes required
4. Data should be accurate and kept up-to-date
5. Data should not be kept for longer than is necessary for purpose
6. Data should be processed in accordance with the rights of data subjects under this act
7. Security: appropriate technical and organizational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the EEA unless that country or territory ensures an adequate level of data protection.

3.0 Data Controller

The company's Data Controller is the Office Manager.
The Data Controller is responsible for informing the ICO of any changes to the company's registration with the ICO, for ensuring people are told exactly what information is being collected, and what it's being collected for, and for ensuring people's consent to the company collecting such information is obtained.
The Data Controller must ensure that if the company buys in a mailing list, the information for any other purpose than the original intention specified.
The Data Controller must ensure that the principles of this policy apply when data is taken out of the office.

4.0 Subject Access Requests

Individuals whose information is recorded have a right to see what data is being kept on them and for what purpose. Information must be provided promptly and within no longer than 40 calendar days of receiving a request. The company reserves the right to charge a fee of £10 (this is the current statutory maximum set by Parliament) to cover the administration of such a request.
Any requests should be directed to the Data Controller.

5.0 Working from Home and Phone Calls

Any staff working from home must agree to keep any work taken home relatively secure, to return all work-related material upon the completion/termination of their contract; and inform the Data Controller promptly if information or data may have got into wrong hands (eg laptop, memory stick, CD ROM, DVD or paperwork has been lost or stolen).
Home computers should have records removed once project/work records are no longer needed at home.
If working on something at home and at work, staff must keep both sets of information up to date. Line managers will keep records of which staff under their supervision take work home.
Calls to the office landline are recorded and are kept secure where only the company's Data Controller can access the information. Recorded calls are kept in accordance with the Eight Data Protection Principles.

6.0 Security Statement

The company has taken measures to guard against unauthorized or unlawful processing or personal data and against accidental loss, destruction or damage.

- This includes:
- Adopting an Information Security Policy (this document is that Policy)
- Taking steps to control physical security - personal records and information are kept in locked cabinets within locked offices.
- Taking steps to control access to electronic information - individual passwords for each user accessing the server, with restricted access to accounts and personnel files.
- Establishing a Business Continuity Plan (regular back-ups of data are taken).
- Awareness training for all staff on this policy and related procedures as relevant Detecting and investigation breaches of security should they occur

7.0 Retention

The company has specified retention periods and the archive and disposal process within our management system procedures, and these must be adhered to.
However, on occasion, we may need to retain information for a longer period, e.g. where a law enforcement body is investigating a crime and ask for it to be preserved, to give them opportunity to view the information as part of an active investigation.

8.0 Monitoring and Review

The company will carry out an internal audit at least annually to ensure that the Eight Data Protection Principles and this policy are being adhered to. This will form part of the internal audits of our management system.
The arrangements in place to implement this policy form part of the company's day to day operational procedures and as such are reviewed on a continuous basis.
Where opportunities for improvement are identified they will be tackled promptly, with sufficient resources, to ensure that they are adequately dealt with, implemented and briefed in to all employees.
This policy will be formally reviewed on an annual basis.

The CRAIN Notice is a data protection transparency document that was worked on by the industry with the blessing of the ICO. Our Compliance Dept. require the link to the CRAIN Notice to be included in your Privacy Policy.

> *'In order to process your application, we will supply your personal information to credit reference agencies (CRAs) and they will give us information about you, such as your financial history. We do this to assess creditworthiness and product suitability, check your identity, manage your account, trace and recover debts and prevent criminal activity. We will also continue to exchange information about you with CRAs on an ongoing basis, including about your settled accounts and any debts not fully repaid on time. CRAs will share your information with other organisations. The identities of the CRAs, and the ways in which they use and share personal information, are explained in more detail at http://www.experian.co.uk/crain/index.html.'*