CAN – DATA PROTECTION POLICY

Both CAN Geotechnical Ltd and CAN Structures Ltd are registered under the General Data Protection Regulations / Data Protection Act.

1. Purpose

1.1 CAN is required to process relevant personnel data regarding staff as part of its operation, and shall take all reasonable steps to do so in accordance with this policy, and the General Data Protection Regulations (GDPR).

1.2 This Policy is subject to all the laws, rules and regulations that CAN is governed by. In the event this policy allows the exercise of discretion, such discretion must be exercised within the confines of the organisation's statutory obligations and must not contravene any of its legal, accounting or other regulatory requirements.

1.3 For the purpose of this policy, Personal Data is "any information relating to an identified or identifiable natural person (Data Subject)".

2. Scope of this Policy

2.1 The scope of this policy covers all processing activities and supporting Information Systems involving personal data. This may include data in physical form, stored in a relevant filing system.

2.1 The scope of this policy covers all employees, contractors, third parties, processors or others who process personal data on behalf of CAN.

3. Requirements

3.1 The Six Principles – Protecting Data

GDPR has six fundamental principles which underpin how CAN controls and/or processes data:

These are:

- **Processed lawfully**, fairly and in a transparent manner.
- **Collected** for specified, explicit and legitimate purposes.
- **Adequate**, relevant and limited to what is necessary.
- **Accurate** and, where necessary, kept up to date.
- **Retained** only for as long as necessary.
- **Processed securely** in an appropriate manner to maintain security.

3.2 Personal data we may need

We may collect and process the following examples of personal information, although we may, at times, need to collect other information not listed below:

- Name and contact information (address, email addresses, telephone numbers)
- Information relevant to our HR functions (National Insurance Number, Passport Number, etc)
- Information to enable us to pay salary (and necessary deductions)
- Information regarding qualifications, skills and expertise.

We may process this information to:

- Carry out statutory functions (ie. payment of wages)
- Keep Data Subjects up to date with changes to CAN's Integrated Management Systems
- Conduct investigations

3.3 The Eight Rights

We recognise that a Data Subject has the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

3.4 Rights of Access to Information

Data Subjects have the right of access to information held by CAN (subject to the provisions of the GDPR and the Freedom of Information Act). Any Data Subject wishing to access their personal data should put their request in writing to the Managing Director. Reasonable steps shall be taken to verify the identity of the Data Subject prior to providing access to their personal data. We would then respond to a request within 30 days. Access requests will not incur a charge.

3.5 Accuracy

CAN will endeavour to ensure that all personal data held in relation to all Data Subjects is accurate. However, Data Subjects must notify CAN of any changes to information held about them.

3.6 Data Security

CAN will take appropriate technical and organisational steps to ensure the security of personal data. All staff are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, all personal data.

In most cases, personal data must be stored in appropriate, secure systems and be encrypted when sent off-site.

3.7 External Processors

It may be necessary for CAN to share some personal data with third parties (training organisations, for example). This is done so in line with the GDPR and the third party receiving personal information will be required to protect information in line with the GDPR.

3.8 Retention of Data

CAN may retain data for different periods of time for different purposes as required by statute or best practice. Legal processes or other statutory obligations may also necessitate the retention of certain data. However, it will not be kept for longer than is necessary.

3.9 Destruction of Data

When data is destroyed, it will be destroyed securely in accordance with best practice.

3.10 CCTV

CAN owns and operates CCTV at both the Chesterfield and Northfleet offices. This is for the purposes of crime prevention and detection, and safeguarding.

Images are not generally retained as part of this system, unless required following criminal activity.

4. Roles and Responsibilities

4.1 The Board has overall responsibility for this Policy.

4.2 Senior Management shall ensure appropriate resources are made available to support the implementation of this policy.

4.3 Internal Auditors shall provide Directors with assurance that CAN is adhering to the requirements of this policy.

5. Approvals and Review

This Policy shall be reviewed annually by the Managing Director (or in line with changes in Legislation, whichever is sooner).

Signed: 

Position: Managing Director

Date: 9th March 2020 Review date: 9th March 2021