General Data Protection Policy

1.0 Introduction

1.1 Anglian Excavations Limited is required to comply with the General Data Protection Regulations 2018. The organisation is required to gather and hold information about individuals that:

- attend an SPA MPQA training course
- show an interest in employment
- information on customers and suppliers
- employees and other people connected to the organisation

This policy lays down the approach to how data must be obtained, handled, securely stored and disposed of to meet the organisation's duty under the General Data Protection Regulations (GDPR) 2018.

2.0 Scope

2.1 This GDPR policy demonstrates Anglian Excavations Ltd commitment and transparency in meeting the new requirements:

- protecting the rights of staff, customers and suppliers
- how it collects, stores and manages individual's information
- reduces the risk from possible data breach

2.2 The regulations describe how an organisation must obtain, handle, securely store and dispose of personal information. The regulations apply whether the information/data is stored as a hard copy or electronically.

2.3 All data on individuals will be collected legally and with the consent from the individual(s). The data must also be:

- relevant
- protected
- not shared with any other party without their permission
- not to be held for longer than is necessary
- destroyed on request
- be presented on request to the relevant individual (free of charge)

3.0 Data & Storage

3.1 The organisation holds relevant data on its employees to ensure that the individual is legitimately identifiable and legally permitted to work in the UK. This data includes:

- name of the individual
- home address
- national insurance number
- passport and/or driving licence details
- email address
- telephone number (landline and/or mobile)
- any other relevant data

3.2 When data is obtained on an individual, it must be with their permission. The individual must be informed that the organisation will keep this data and explain what that data is used for.

3.3 The above data will be kept securely at the Rattlesden office and only those who are authorised can access the information.

3.4 Office staff should ensure that no personal data is left visible on a computer screen when the equipment is left unattended.

3.5 Hard copy personal data must not be left unsecure within the office for 'others' to see. Only authorised staff may have access to staff personal data and information.

3.6 Personal data should not be shared informally with others and where possible, it should not be sent via an email which is not secured outside of the organisation.

3.7 Office staff must not save copies of personal data to their own computer system.

3.8 The organisation also holds data appertaining to its customers and service providers however, this data is limited and only relevant to the business activity. This includes:

- company name
- the relevant contact (individual(s))
- postal address
- email address
- telephone numbers – landline and/or mobile
- banking details are held for payments (secured banking protocol)

3.9 Staff should take the opportunity to update customer and service providers (relevant) data, when speaking with them.

3.10 Data stored on individuals who have attended an SPA training course will be securely stored in both paper and electronic form. This information will be kept for three years and three months, as per the SPA's licence agreement. After this period the data will be destroyed in line with the requirements of this policy.

3.11 Where data is stored electronically it will be protected from unauthorised access, accidental deletion and malicious hacking attempts.

4.0 Security

4.1 The organisation's IT service provider will ensure the that IT software systems is updated and maintained to a recognised acceptable security standard.

4.2 Where data is stored electronically, the information must be protected from unauthorised access, accidental deletion and any hacking attempts.

4.3 The office computer system is managed by one primary server which is password protected. This is managed and safeguarded by the Office Administration Manager.

4.4 Any hard copy data that falls under the GDPR will be stored safely within the main office, in locked cabinets.

4.5 Electronic data will be backed up at the end of each working day. Backed up information will be stored off site in line with the organisation's businesses continuity plan.

4.6 The server is protected with security software and suitable firewalls managed by external IT service provider.

5.0 Disposal

5.1 Any hard copy personal data that has either expired or no longer required should be disposed of securely for example, shredded in the main office.

5.2 At times the organisation will have to safeguard expired information (store appropriately), where the information is necessary for other regulatory bodies i.e. the Health and Safety Executive.

6.0 Request For Information

6.1 Employees or external SPA trained delegates are entitled to request what information is being held about them by Anglian Excavations Limited. If the employee wishes to access this information they must:

- formally write to the organisation for the attention of the CEO
- clearly state their request

6.2 The organisation will respond to individual's data requests within one calendar month and issue the information free of charge.

6.3 The Administration Manager will always verify the identity of the person making the request, before handing over any personal information.

7.0 Responsibility

7.1 Anglian Excavations Limited staff have a responsibility for ensuring that data is collected handled stored and disposed of appropriately. The administration and management team must ensure that data is handled in line with GDPR.

7.2 The CEO is responsible for ensuring that the company meets its legal requirements under GDPR and will ensure an annual review is undertaken to assess:

- data storage procedures
- authorised persons for data handling
- any individual requests about data stored about them
- data is found to be no longer required and should be disposed of responsibly

Signed:_____
Chris Lee

Position: Chief Executive Officer
Date: January 2021