STRATEGIC GROUP POLICY SGP001

DATA PROTECTION

LEADERSHIP

Written by: Liam O'Loughlin

Date: 07/02/2022

Revision: 05 **Doc Ref:** SGP001 **Reviewed by:** Andrew Smith

VISION:

Our Vision: "To ensure that our data, and the data of the people we work with, is protected from misuse and is given sufficient sensitivity where required"

We are realising our Vision by working with leading experts to ensure our systems are secure and can only be operated in protected and legal ways.

COMMITMENT:

Arthur Civil Engineering Ltd are committed to protecting Client and Third-Party data. We expect our employees to ensure that they comply with this policy in the interest of protecting our Client, Third-Party and their work colleagues' data.

We expect all of our employees to be familiar with key Data Protection rules and terminology – not just as 'data subjects' but also as 'data handlers'. We have a separate **Privacy Notice** which relates to personal information in the context of employment. This Data Protection Policy is concerned primarily with **client and third-party data** – which we all have a duty to protect.

To support this statement, in 2019/20 Arthur Civil Engineering Ltd will:

- Assign individuals to take responsibility for Data Protection – and these are the Directors of the Company;
- Instruct all employees and contractors who manage and handle personal data so that they understand their safeguarding duties and obligations;
- Regularly assess and evaluate our methods of handling personal data;
- Obtain personal data only for specified and lawful purposes;
- Can account for the accuracy of the data and, where required, keep it up to date;
- Do not keep personal data for longer than is necessary;
- Process personal data in accordance with the rights of data subjects under the General Data Protection Regulation 2018;
- Take measures to prevent unauthorised or unlawful processing of personal data and the accidental loss or destruction of, or damage to, personal data;

- Do not transfer personal data to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

RESPONSIBILITY:

The Directors of Arthur Civil Engineering will:

- Monitor compliance with this Data Protection Policy.
- Ensure Arthur Civil Engineering Ltd works with clients and their Data Protection Policies.
- Communicate this Policy to their employees to ensure awareness throughout the Company.
- Ensure sufficient provision of resources is made in order to implement the requirements of this Policy.

All Employees of Arthur Civil Engineering must ensure they:

- Stop and consider whether they should be accessing or disclosing personal data before they do so;
- Make sure that they have verified that the person they are passing data on to is who they say they are and that they are authorised to receive it;
- Do not discuss information about clients, colleagues and third parties with unauthorised colleagues, family or friends, or Arthur Civil Engineering Ltd clients;
- Do not access Arthur Civil Engineering Ltd business records containing personal data other than for a specific business purpose. This may also be an offence under the GDPR and the Company may be prosecuted by the ICO;
- Avoid providing any specific detail about individuals that might lead to their identification when using information for reports or monitoring purposes unless they have given written permission for it to be used;
- Do not express unsubstantiated personal opinions in file notes, e-mails or other means of communication; individuals may have a right to see the information and may exercise that right;
- Give careful consideration to the use of e-mail distribution lists and the blind carbon copy (BCC) option especially when sending out e-mails to large numbers of recipients (i.e. clients, colleagues, or third parties);
- Always remember to consult their manager, and if necessary one of the Directors for their input before starting any projects involving the processing of personal data;
- Always consider data security and the risks associated with losing personal data, before downloading/printing any personal data;
- Never share their computer password or write it down; doing so could result in the unauthorised accessing of personal data and, therefore, a serious security breach;
- Always lock their screen when leaving their computer – even if it's only for a few minutes – and remember to log off at the end of the day;
- Never work on any Arthur Civil Engineering Ltd data in a public place including use of mobile phones and laptops;
- Take care not to leave documents containing personal data on the printer, photocopier or scanner (please note fax machines should not be used to transmit personal data as the ICO consider it out-dated and unsecure);

- Make sure that personal data cannot be seen or accessed by unauthorised individuals either in or out of the office. If sensitive data is taken out of a building, it needs to be in a locked bag. When travelling by car papers must always be transported in the boot of the car. Papers must not be left in the car overnight; when at home in locked bag or secured cabinet;

- Remember to dispose of confidential waste and paper copies containing personal data in special bins or by shredding;
- Ensure personal data extracted for Arthur Civil Engineering Ltd use is stored on encrypted memory sticks or other suitable encrypted storage. Refer to one of the Directors if encryption is required. Data uploaded to any third party web-storage must be treated with the same level of security and permission must be sought in advance of any upload;
- Extract data only with approval from their line manager and be aware that the control of the data whilst extracted is the joint responsibility of the "data extractor" and their manager.

APPROACH:

Transfer of Personal Data to a Third Party

We require all employees to be aware of the following important protocols in the event that **personal** data is transferred to a third party:

- Before personal data is transferred, a Non-Disclosure Agreement (NDA) or Data Processing Agreement (DPA) should be in place between Arthur Civil Engineering Ltd and the third party. Alternatively, the third party may present terms to Arthur Civil Engineering Ltd that satisfy the requirements of this clause.

- The agreement between the parties, whatever its form, should clearly state the third party's obligation to treat the data in accordance with the provisions of the General Data Protection Regulation.

- NDAs/DPAs are managed by our Managing Director and employees may assume that these are in place only when a third party is formally introduced to the Company. If you have any doubt whatsoever about the relationship that exists between Arthur Civil Engineering Ltd and a third party, please speak directly to a Director and do not transfer any personal data to the third party until you have done so.

- Please be aware that personal data transfer beyond the UK and EU is subject to special arrangements. As above, if you have any doubt whatsoever about the relationship that exists between Arthur Civil Engineering Ltd and a non-UK or non-EU third party please speak directly to one of the Directors and do not transfer any personal data to the third party until you have done so.

- If you are responsible for transferring data to a third party, please be aware of the following precautions:

i. If data is sent via a courier the intended recipient must be advised when to expect the data;
ii. The recipient must confirm safe receipt as soon as the data arrives;
iii. Data must not be transferred outside of the Company network other than to an authorised recipient, such as a client or contractor. **If sent via the internet, all personally identifiable data must be either password protected and/or encrypted;**
iv. Never transfer personal data to your personal cloud account, memory stick, email account or similar. This may result in disciplinary action and/or enforcement action by the Information Commissioner's Office.

External Transfer of Personal and Sensitive Data
Principle

The following guidance sets out how personal and/or sensitive information should be processed to ensure that our clients', colleagues' or any third party's data is in no way compromised. This includes the transferring, storage and disposal of information and information held on our behalf by contractors. If you have personal information that is currently stored or transferred insecurely, you must secure it immediately.

Transferring Personal and/or Sensitive Data by Email

Please observe the following essential protocols for personal and/or sensitive data transfer via email:

- Sensitive information (see 'definitions' below) relating to a single individual can be sent via email attachment to the subject of the information if they have requested it to be sent by email or with their agreement and it is encrypted. The exception to this is when the individual has stated that they want to receive the information without encryption. A record must be kept of this request;

- Documents containing sensitive personal information cannot be sent to third parties without encryption and should not be contained within the body of an email but attached as an encrypted document;

- Care should be taken when addressing email messages to ensure a correct, current address is used and the email is only copied to those with a legitimate business interest;

- If information is transmitted and not received by the intended recipient, check that contact details and email address are correct for the receiving party before re-sending;

- Consider the impact on individuals of the data being lost or misdirected. Where information is provided in bulk or where the information is of a sensitive nature make an assessment on the protection to be applied. If in doubt, send information in an encrypted attachment to the email;
- Avoid putting sensitive personal information about more than one person in an email as this will lead to difficulties in maintaining accurate and relevant individual client or staff records;

- When transferring data be aware of who has permission to view your emails or who might be able to view your recipient's inbox;

- Where email and personal data are stored or accessed on any mobile device, such device must be protected with a password/PIN/finger print or other secure login means.

Dealing with a Data Breach

If a data breach is suspected staff should **immediately** notify one of the Directors. Following notification Arthur Civil Engineering Ltd will take the following actions urgently:

- Implement a recovery plan, including damage limitation;
- Assess the risks associated with the breach;
- Inform the appropriate people and organisations that the breach has occurred;
- Review our response and update our information security.

Breach of the Arthur Civil Engineering Ltd Data Protection Policy

In the event that an employee fails to comply with this Policy, the matter may be considered as misconduct and dealt with in accordance with Arthur Civil Engineering Ltd Disciplinary Policy and procedure.

Removable Media

- In line with our commitment to safeguard not only our own but our clients' and other third parties' confidential information, we require all employees to conform with our policy on removable media. For clarity, 'removable media' will include – amongst other things - CDs, DVDs, optical disks, external hard drives, USB memory sticks (pen drives or flash drives), media card readers, Smart cards, SIM cards, and digital cameras. Misuse of removable media can result in:
  i. Disclosure of protected and restricted information as a consequence of loss or theft.
  ii. Contamination of Company networks or equipment through the introduction of viruses.
  iii. Through the transfer of data from one form of IT equipment to another.
  iv. Potential legal action against the Company or individuals as a result of information loss or misuse.
  v. Significant reputational damage for Arthur Civil Engineering Ltd.

- The only equipment and media that should be used to connect to Company equipment or the network is equipment and media that has been purchased by the Company and approved by the one of the Directors.

- Data stored on removable media must be backed up / copied on the system or a networked computer.

- All removable media devices must be encrypted / secured.

- Any suspected breaches of information security (loss / damage / theft) must be immediately reported to one of the Directors.

- No third party may receive data or extract information from the Company's network, information stores or IT equipment without the explicit agreement of one of the Directors. Furthermore, the third party will be required to sign a Non-Disclosure and Confidentiality Agreement and must be made fully aware of our Data Protection Policy.

- Damaged or obsolete removable media must be securely disposed of or erased to avoid data leakage.

DEFINITIONS:

Personal information/data relates to a living individual who can be identified from the information (or from that information and any other information in the possession of Arthur Civil Engineering). This includes both factual information and opinion as expressed by a third party.

Sensitive personal information / data attracts additional protection in law and is considered by the Information Commissioner's Office (ICO) to be any data that could lead to the identification of a person and is overtly personal in nature. Example of this would include personal data consisting of information such as:

- The racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sex life / sexual orientation
- Commission or alleged commission of any offence
- Any proceeding for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of court in such proceedings
- Details of bank account, national insurance number, any ID details such as passport or driving licence, etc.

A data **record** can be in computerised and / or manual form. It may include such documentation as:

- Hand written notes
- Letters to and from Arthur Civil Engineering
- Electronic records
- Printouts
- Photographs
- Videos and tape recordings.

Data Subject means an individual who is the subject of personal data.

Data Handler or **Data Extractor** is any party who is given access to and transfers, stores, or destroys 'data'.

REVISION STATUS:

	Rev.	Date	Description if Addition (A), Deletion (D) or Substitution (S)	Approved by:
1.1	01	05.07.2018	Written by Liam O'Loughlin	Andrew Smith
1.2	02	05.07.2019	2019 Review	Andrew Smith
1.3	03	05.07.2020	2020 Review	Andrew Smith
1.4	04	17.05.2021	2021 Review	Andrew Smith
1.5	05	07.02.2022	2022 Review	Andrew Smith

The information contained in this Policy applies to all employees of Arthur Civil Engineering Limited ('Arthur Civil Engineering Ltd' or 'the Company') subject to any qualifying conditions described. This policy should be read in conjunction with your Contract of Employment and the Company Handbook. The Company may amend and extend the contents of this document at any time, subject to statutory and/or operational requirements. If you require any clarification in respect of this Policy, please speak in the first instance to one of the Directors.