SEDDON GROUP LTD
DATA PROTECTION POLICY

1. Purpose of the Policy

To communicate the policy of Seddon Group Limited and its subsidiary companies (the Company) to comply with it's obligations under the Data Protection Act (2018) (the Act) and the General Data Protection Regulations 2018 (the GDPR) (and any subsequent enactments) (together the Law).

2. Policy Statement

The Law sets out the conditions under which an organisation may process personal data, and, provides individuals with rights with regards to how their personal data is processed (ie what and how it is collected, the purposes for which it is used for, how it is stored and handled, for how long it is retained, and, how it is disposed of).

As part of its business activities the Company will process data in respect of its employees, suppliers, contractors, customers, services providers and others with whom it communicates. During your employment you may encounter or need to use confidential information about other individuals and you must comply with the Law. Individuals who are protected under the Act are known as 'data subjects'.

The Act, updated by the GDPR, sets out the legal principles relating to the handling of personal data which may be stored on computer or in manual records. If you are in any doubt about what information you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from your line manager or the Legal Department. You can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Law. A breach of the Law by you will be dealt with under the Company's disciplinary procedures. If you access another's personal record without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal. This policy does not form part of your contract of employment and may be amended at any time. By signing your contract of employment, you have expressly consented to the Company holding, limited appropriate sensitive personal data about you.

3. Data Protection Definitions

Data is information which is stored electronically or in certain paper based filing systems.

Data Subjects for this policy includes all living individuals about whom Seddon hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or sexual life, or about any legal proceedings or offences committed or alleged to have been committed by the individual. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person.

Data Controllers determine the valid and lawful purposes and means of processing the personal data.

Data Users include employees whose work involves using personal data.

Data processors include any person who processes personal data on behalf of a data controller.

Processing is any activity that involves the use of data which includes obtaining, recording or holding the data, or carrying out an operation or series of operations on the data including organising, amending or retrieving, using, disclosing, erasing or destroying it. Processing must be for a demonstrable valid and lawful purpose and includes transferring data to a third party

4. The Data Protection Principles

These were set out as 8 principles under the DPA but have been updated by the GDPR Article 5 as follows and the Company and all its employees must comply with these principles:

Data must be:
Principle 1 Processed fairly, lawfully and transparently
Principle 2 Collected for a specified, explicit and legitimate purpose
Principle 3 Adequate, relevant and limited to the purpose
Principle 4 Accurate, and where necessary up to date
Principle 5 Kept for no longer than is necessary for the purpose
Principle 6 Processed in manner to ensure appropriate security

The GDPR principles state that personal data must be:

4.1 Processed fairly, lawfully and transparently (Principle 1)

The Law is not intended to prevent the processing of personal data but to make sure it is done fairly and without adversely affecting the right of the individual. To ensure that data is processed in a fair and transparent manner the data subject must be given certain information:

- The identity of the Data Controller (which in this policy is Seddon Group Limited)
- The purpose or purposes for which the data will be used, and;
- The identities of anyone to whom the data may be disclosed or transferred

Data must not be processed unless the individual has given its consent or the processing is specifically authorised by the Act. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

- race or ethnic origin
- political opinions and trade union membership
- religious or other beliefs
- physical or mental health or condition
- sexual orientation
- criminal offences, both committed and alleged
- genetic and biometric data

4.2 Processed for a specified, explicit and legitimate purpose (Principle 2)

The data can only be collected for a specific purpose for which the individual was made aware. Any change in the purpose of collection must be first notified to the individual prior to any use of the data.

4.3 Adequate, relevant and limited to the purpose (Principle 3)

The Company will only obtain and retain personal data if there is a clear reason for collecting and retaining the data and the individual is clear about the purpose for storing the data.

4.4 Accurate and where necessary up-to-date (Principle 4)

The Company will review files held of a personal nature to ensure they do not contain out of date information. The information held should be up to date and must be refreshed and updated regularly. If your personal information changes you must inform the People Department of any changes as soon as practicable so that the records can be updated. The Company cannot be held responsible for any out of date information if you have not notified the relevant change.

4.5 Kept for no longer than is necessary for the purpose (Principle 5)

Personal data will be kept for no longer than is necessary for the purpose. The Company will keep personnel files for no longer than seven years after termination of employment. Data relating to unsuccessful job applications will not be retained for more than six months. Other categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold will be destroyed after six months.

4.6 Processed in manner to ensure appropriate security (Principle 6)

Maintaining data security means guaranteeing confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised may access it.
(b) **Integrity** means that personal data should be accurate and suitable for the consented purpose for which it is being processed.
(c) **Availability** means that authorised users should be able to access the data if they need it for the authorised purposes. Personal data must therefore be stored on the central computer system and not on individual PCs.

Security measure include:

(a) **Entry Controls.** Any stranger seen in entry-controlled areas to be reported.
(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind.
(c) **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-Roms and pen drives should be physically destroyed if no longer required.
(d) **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and if used out of the office in public places should have screen shields in place. Computers to be logged out or locked when left unattended.
(e) **System security.** Careful consideration should be paid to restricting access and password protecting personal data.

The Company has systems in place to maintain and protect the security of data held electronically including:
• Firewalls
• Virus checkers
• The facility to password protect documents and data bases
• Data encryption

5. Off Site and Homeworking

The Company understands that remote working from either home, on site or in public places is the normal modern way of working and the Company encourages mobile working where this is appropriate and the most effective way of carrying out their employment. Each individual must comply with this policy and ensure that personal data is maintained securely in compliance with the Law. Only Seddon supplied portable storage devices (including USB pen drives) should be used for storage and transport of confidential data that leaves the Seddon secure environment. These devices are protected by security passwords, virus checkers and firewalls.

6. Right to Access Personal Information

An individual has the following rights to:

(a) Request access to any data held about them by the Company.
(b) Prevent the processing of their data for direct marketing purposes.
(c) Request that inaccurate data is amended.
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

An individual has the right, on request, to receive a copy of the personal information held by the Company including their personnel file, and to request that any inaccurate data be corrected or removed. You have the right:

• to be told clearly and concisely by the Company what information they hold and for what purpose your personal data is being processed.
• to be given a description of the data held and the recipients to whom it may be disclosed.
• to have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data.
• to be informed of the logic involved in computerised decision-making.

Upon written request, the Company will provide a statement regarding the personal data held about you. The information must be provided without delay and in any event within one month of receipt of the request.

This period can be extended by a further two months where requests are complex or numerous provided you notify the individual within one month and explain why the extension is necessary.

7. Right to Access Personal Information

The Company will uphold its obligations under the Law in relation to the principles governing the collection and maintenance of personal data. Any member of staff who receives a data protection related complaint or feels that there has been a breach in relation to data protection must report the matter to their line manager and or the Legal Department at the earliest opportunity.

Examples of data protection related complaints include:

- inaccurate personal data
- unlawful access to or disclosure of personal data
- accidental loss destruction damage or modification of person data
- the unlawful retention or disposal of personal data

Once the Company is aware of the complaint then they will obtain all the information they require to enable them to fully investigate the complaint in accordance with the **Data Protection Complaint Protocol**. If the matter is not resolved to your satisfaction, it should be escalated to the Director of Legal, Risk and Compliance.

8. Your Obligations in Relation to Personal Information

You should ensure you comply with the following guidelines always:

- Do not give out confidential personal information except to the data subject. Information should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.
- Be aware that those seeking information sometimes use deception to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly, before releasing personal information by telephone.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- If you receive a request for personal information about another employee, you should forward this to the People Department responsible for dealing with such requests.

9. Breach Notifications

GDPR imposes a duty on all organisations to report certain types of breach to the Information Commissioner's Office (the ICO) being the supervisory authority and in some cases the individuals affected.

A data breach means a breach of security leading to destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach can be more than just losing personal data.

A reportable breach will be reported to the ICO within 72 hours of Seddon becoming aware of it.

A reportable breach is one which is likely to result in a risk to the rights and freedoms of an individual and which if not addressed might have a significant detrimental effect to the individual which might result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. An individual must be notified if the breach is likely to result in high risk to the rights and freedoms of the individual and the threshold for individual notification is higher than the obligation to notify the ICO.

Any data breach that arises will be reviewed to decide if the breach is notifiable to either the ICO and /or the individual. Any notifiable breach will contain the following information:

- The categories and number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- Details of the contact within Seddon to communicate with;
- A description of the likely perceived consequences of the data breach;
- The measures taken or proposed to be taken to remedy and mitigate the impact of the breach.

10. Compliance Monitoring and Review

This policy is reviewed by Seddon Group Board and the Legal Department to ensure that it remains up-to-date and compliant with the Law. The Company will ensure that regular training is provided to senior management and its employees to make sure that they understand the Law and are familiar with their obligations under the policy.

Seddon are accountable for compliance with the Law and must be able to demonstrate compliance. Monitoring and checks will be carried out to ensure compliance and an audit programme will introduced to demonstrate compliance.

Seddon will maintain internal records of its processing activities which include:

- Details of the processing activities that take place;
- Description of the categories of individuals and categories of the personal data held
- Categories of recipients of personal data
- Retention schedules
- Details of technical and organisational security measures

11. Retention Statement

The Company policy in relation to data retention is that personal data shall not be kept longer than is necessary for the purpose.

The Company will retain data and records as required per the guidance periods shown in Appendix A. Reasons for retention will include the following:

- Statute requires retention for a set period (see Appendix A).
- The record contains information relevant to legal action which has been started or is in contemplation.
- Records and information should not be amended or disposed of until the threat of litigation has been removed.
- The records are maintained for retrospective comparison.
- Employee records can be retained for the purposes of managing civil claims.

12. Destruction and Disposal Procedures

The Company will ensure that that all data is disposed of properly and all information of a confidential or sensitive nature on paper card microfiche or electronic media will be securely destroyed when no longer required.

- A record of externally archived documents must be maintained.
- Any confidential or sensitive paper data should be disposed of by shredding
- All other paper can be disposed of in boxes or bins provided in offices for environmentally friendly disposal of non-confidential and non-sensitive paper waste.
- Media being destroyed because of damage or because its obsolete should be destroyed by being cut into pieces before disposal.
- Where discs, tapes, DVD or CD Rom are being used to supply data to third parties they should, at the very least, be reformatted before the files are saved on to it.
- Ensure destruction of back-up copies of any data.

COMPLIANCE WITH THE LAW IS YOUR RESPONSIBILITY. IF YOU HAVE ANY QUESTIONS OR CONCERNS ABOUT THE INTERPRETATION OF THIS POLICY CONTACT THE PEOPLE DEPARTMENT.