DATA PROTECTION & ONLINE SECURITY POLICY

Policy Reference Number:	KRD-POL-DATA-2110-B
Revision Date:	18 October 2022
Review Date:	18 October 2023
Approved By:	Rob Kennedy
Signed:	

This policy statement is supplemented by other business policies, core values and mission statement which are available on our company website www.kennedyredford.com

DATA PROTECTION & ONLINE SECURITY

Kennedy Redford Limited shall protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our clients. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

Personal Data

Personal data is defined by the Data protection Act 2018 as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

In accordance with the Data protection Act 2018, Kennedy Redford Limited shall ensure that Personal Data shall be:

- Processed fairly and lawfully.
- Obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes.
- Adequate, relevant and not excessive with respect to the purposes for which it is processed.
- Accurate and, where appropriate, kept up to date.
- Kept for no longer than is necessary for light of the purposes(s) for which it is processed.
- Processed in accordance with the rights of data subjects under the Data Protection Act 2018.
- Protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures. And,
- Kept secure to prevent the transfer to a country or territory outside of 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.

In accordance with the Data protection Act 2018, Kennedy Redford Limited commit to ensuring that all data subjects have the right to:

- Access a copy of their personal data held by the Company by means of a Subject Access Request.
- Object to any processing of their personal data that is likely to cause (or that is causing) damage or distress.

- Prevent processing for direct marketing purposes.
- Object to decisions being taken by automated means (where such decisions will have a significant effect on the data subject) and to be informed when any such decision is taken (in which case the data subject has the right to require the data controller (by written notice) to reconsider the decision.
- Have inaccurate personal data rectified, blocked, erased or destroyed when requested.
- Claim compensation for damage caused by the Company's breach of the Act.

Data protection procedures

Kennedy Redford Limited shall ensure that all of its employees, agents, contractors, or other parties working on behalf of the Company comply with the following when working with personal, sensitive or data relating to other Clients or Customers:

- All emails containing data must be encrypted.
- Data shall only be transmitted over secure networks with a firewall installed – transmission over unsecured networks is not permitted in any circumstances.
- Data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- Data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
- Where Personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or posted using a track and trace service with a signature required from the named recipient.
- No personal data may be shared informally, and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested.
- Data must be handled with care at all times and should not be left unattended or on view to unauthorized employees, agents, sub-contractors or other parties at any time.
- If data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
- Any unwanted copies of data (i.e. printouts or electronic duplicates) that are no longer needed should be disposed of securely. Hardcopies should be shredded, and electronic copies should be deleted.
- No data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise.
- All personal data stored electronically should be backed up and encrypted.

Password Management

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and or exploitation of company resources. All users, including contractors and vendors with access to company data, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised.
- All passwords should be at least 8 characters in length, must contain a combination of uppercase and lowercase letters, numbers, and symbols, must not be a common word or name, should not be shared with any other account password.
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.
- Passwords should not be stored in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Users should NOT use the "Remember Password" feature of applications (for example, web browsers).

Organisational Measures

Kennedy Redford Limited Have appointed Robert Kennedy as its Data Protection Officer with the specific responsibility of overseeing data protection and ensuring compliance with this Policy and the Data protection Act 2018.

The Data Protection Officer shall ensure that:

- All employees, agents, contractors, or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company's responsibilities under the Act and under this Policy and shall be provided with a copy of this Policy.
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to and use of personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The Performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract.

Access to personal data (Subject access request)

Any Person that Kennedy Redford Limited hold personal data about may make a subject access request at any time to find out more about the information that Kennedy Redford Limited hold about them.

Subject access requests should be made in writing and addressed to the company director and should be clearly identified as a subject access request.

The subject access request must make it clear whether it is the person themselves that is making the request or whether it is a person acting on his or her behalf. In either case, proof of identity must be provided. If the subject access request is made on another's behalf, the individual making the request must provide clear evidence of their authorised capacity to act on behalf of the data subject.

Upon the receipt of the Subject access request, Kennedy Redford Limited shall have a maximum period of 40 calendar days within which to respond fully, although an acknowledgement should be received within 10 working days.

The following information will be provided with:

- Whether or not the Company holds any personal data on the Person requesting the Subject access request.
- A description of any personal data held on the person.
- Details of what that personal data is used for.
- Details of how to access personal data and how to keep it up to date.
- Details of any third-party organisations that personal data is passed to. And,
- Details of any technical terminology or codes.

Notification to the information commissioner's office

As a data controller, the Kennedy Redford Limited is required to notify the Information Commissioner's Office that it is processing personal data.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place. The Data Protection Officer shall be responsible for notifying and updating the Information Commissioner's Office.