Bremner and Co

Data Protection policy

IT and Information Security policy – *see employee handbook.*

Aim & Purpose of the policy

This policy relates to General Data Protection Regulation (GDPR) and the importance of Compliance within the company.

The Company needs to keep certain information on its employees, volunteers and associates, to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations.

The Company is committed to ensuring any personal data will be dealt with in line with current data protection laws (General Data Protection Regulation (GDPR) and the Data Protection Act 2018). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the Company.

This policy applies to all personal and sensitive personal data collected and processed by the Company in the conduct of its business, in electronic format in any medium and within structured paper filing systems either stored on site or remotely.

Types of information processed

The name of the data controller within the company is Bremner and Co registered with the Information Commissioner's Office (ICO) to process personal data in order to promote the interests of the company; to manage employees and associates; personal data may also be collected as part of consultancy and research projects undertaken by the Company.

The Company notifies and renews its notification on an annual basis as the law requires. Any interim changes are notified to the Information Commissioner within 28 days.

Personal data is processed for past, current and prospective:

- Employees
- Associates
- Supporters/Donors
- Complainants/enquirers
- Service users
- Project beneficiaries
- Funders
- Suppliers
- Representatives of other organisations
- Research participants

Groups of people who will process personal information are:

- Employees
- Associates
- Third party suppliers

Personal information is either held in paper-based filing systems or stored electronically.

Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data in the business rests with the Company. In the case of Bremner & Co, this is the Chief Executive Officer.

The Data Controller is responsible for:

- understanding and communicating obligations under GDPR/DPA 2018;
- identifying potential problem areas or risks;
- producing clear and effective procedures**;**
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes.

Data controllers must ensure that any processing of personal data for which they are responsible complies with GDPR/DPA 2018 principles. Failure to do so risks enforcement action and even criminal prosecution. The ICO also has the power to serve a monetary penalty notice on a data controller for breach of the Act.

All employees, casual workers, and associates who process personal information must ensure that they not only understand but also act in line with this policy and the data protection principles.

Bremner & Co is not required to appoint a Data Protection Officer. Therefore, we have taken the decision not to appoint a DPO; however, we note that the company still needs to discharge its obligations under the GDPR and the Data Protection Act 2018. If we task staff or external consultants to support us with data protection, we will ensure that it is clear that they are not a Data Protection Officer as set out in the GDPR.

Policy Implementation

To meet data protection responsibilities all employees, casual workers, and associates will:

- familiarise themselves with this policy and the IT and Information security policy and adhere to them at all times;
- ensure any personal data is collected in a fair and lawful way;
- make individuals aware of the intended use of their data at the point of collection either verbally, written or via direction to the relevant privacy notice;
- ensure that only the minimum amount of information needed is collected and used;
- ensure the information is kept up to date and accurate;
- review the length of time information is held and establish appropriate retention periods;
- ensure personal data that is no longer needed (in line with company retention guidelines) are disposed of effectively and securely;
- ensure personal data are kept securely;
- ensure the rights people have in relation to their personal data can be exercised including opt-outs and 'cease processing' requests;
- be mindful that individuals have the right to see their personal data (e.g. comments sent in emails) and so take care not to record comments or other data about individuals which they would not be comfortable for the individual to see;
- inform the Data Protection Lead in the event of any intended new purposes for processing personal data; no new purpose for processing data will take place until the ICO has been notified of the relevant new purpose and the data subjects have been informed, or in the case of sensitive data, their consent has been obtained;
- report any actual, near miss or suspected data breaches (either accidental or as a result of theft) immediately to the Data Protection Lead for investigation.

The Company will ensure that:

- a nominated lead is responsible for data protection compliance, providing a point of contact for all data protection issues;
- everyone managing and handling personal information is appropriately trained and supported to do so;
- everyone handling personal data knows where to find further guidance;
- adequate security measures are in place to protect personal data;
- any disclosure of personal data will be in line with company procedures;
- queries about handling personal information are dealt with effectively and promptly;
- data protection procedures and guidelines within the Company are reviewed regularly.

Training

Training and awareness raising about the General Data Protection Regulations and the Data Protection Act 2018 and how they are followed in this Company will take place on Induction

Data security

Keeping data properly secure is key in complying with current data protection laws. The Company will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- following UK government Cyber Essentials to ensure safety and security of IT systems including boundary firewalls and internet gateways, secure configuration of hardware and software, password control, malware protection and appropriate patch management/software updates;
- implementation of a robust back-up strategy;
- appropriate electronic storage of personal data with folder access given only to authorised personnel;
- any transfer of personal data from one place to another or storage off site will be done in line with the Organisation's IT and Information Security policy;

Please refer to the Company's IT and Information Security policy for further information and rules on security including the acceptable use of mobile electronic devices.

Any unauthorised disclosure of personal data to a third party by an employee or affiliate is considered a breach of this policy which may result in further action as previously outlined in the responsibilities section of this policy.

Subject Access Requests

Anyone whose personal information is processed by the Company has the right to know:

- what information the Company holds and processes on them;
- how to gain access to this information;
- how to keep it up to date;
- what the Company is doing to comply with data protection laws.

Individuals also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under GDPR/DPA 2018 to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the Data Protection Lead. The Organisation may require proof of identity before access is granted.

The Company will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within the statutory time permitted under GDPR from receiving the written request.

The Company's privacy notice will include a contact address for data subjects to use should they wish to submit a Subject Access Request, or make a comment or complaint about how the Company is processing their data or about the Organisation's handling of their request for information.

Employees and affiliates are aware that in the event of a Subject Access Request being received by the Company all corporate systems including emails may be searched and relevant content disclosed whether marked as personal or not.

Upon receipt of a request the Data Protection Lead must be informed at the earliest opportunity. The request will be assessed and the Data Protection Lead will obtain all relevant information from each department or confirm that none exists, as defined under the GDPR regulations.

Transparency

We will ensure all stakeholders are informed about our processing of their personal data by having the following privacy notices available:

1. General Privacy Notice (available on website at xx
2. Employee Privacy Notice

Review

This policy will be reviewed at 2 yearly intervals to ensure it remains up to date and compliant with the law. This policy was reviewed April 2023

Agreement

This must be signed and returned to the CEO within 1 week of being issued.

I have read and understood the data protection policy and agree to adhere to its contents.

Name and position: ……

Signature: ……..

Date: ……

Definition of Key Terms

Controller – a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Only controllers need to pay the data protection fee.

Processor – a person, public authority, agency or other body which processes personal data on behalf of the controller.

Data protection Lead –responsible for informing them the organisation and advising about their data protection obligations and monitoring compliance with them.

Data subject – the identified or identifiable living individual to whom personal data relates.

Data Protection Impact Assessment (DPIA) – A method of identifying and addressing privacy risks in compliance with data protection laws.