Data Protection Policy
Grangemouth and Bo'ness CAB

Date of last review	**November 2024**
Date of next review	**November 2025**

1. Introduction

During the course of our operations, we are required to gather and use certain information about individuals, to provide services, for employment purposes, and to comply with the Data Protection Act 2018 and UK General Data Protection Regulation ('Data Protection Law') describe how organisations must collect, handle and store personal information.

This policy explains the procedures that must be followed by all Team Members to meet the Bureau's data protection standards and to comply with Data Protection Law.

This data protection policy ensures Grangemouth and Bo'ness CAB follows the data protection principles, which means Grangemouth and Bo'ness CAB processes personal data in a way that:

- Complies with data protection law and follows good practice;
- Is open and fair about how it uses individuals' data;
- Is necessary to achieve a legitimate purpose;
- Ensures it is accurate and up to date;
- Is not excessive, we only keep personal data for as long as we need it; and
- Secure to protect individual's rights and reduce the risk of a data breach.

2. Policy scope

This policy applies to:

- All employees and volunteers, donors;
- All contractors, suppliers and other people working on behalf of the Bureau; and
- Any person or organisation who collects or handles personal data on behalf of Grangemouth and Bo'ness CAB.

It applies to all personal data whether in electronic or paper format that relates to those individuals including:

- Personal data which could identify individuals such as names, postal addresses, email addresses, telephone numbers, financial data, employment information; and
- Special Category data such as race, ethnic origin, religious or philosophical beliefs, trade union membership, genetics, biometrics (where used for ID purposes); health, sex life; sexual orientation, family circumstances and also sensitive data relating to criminal convictions.

3. Roles and Responsibilities

2.1 Everyone

Every team member at Grangemouth and Bo'ness CAB has responsibility for ensuring that personal data is used appropriately and in accordance with the principles of data protection law. Support is available from key team members to assist you with any data protection queries you have. The key point of contact is:

Data Protection Officer/Contact: Thorntons Law LLP
Email address: CABDPO@thorntons-law.co.uk

Everyone should:

- Be aware of, and understand, the data protection principles
- Access personal data only where needed to fulfil their tasks
- Use authorised equipment and follow relevant guidance in compliance with IT policies
- Be aware of data protection procedures including data protection impact assessments, data sharing agreements, data processing agreements, and record of processing activities as it relates to their role
- Request advice from the Data Protection Officer (DPO) if unsure about any aspect of data protection.

2.2 Line Manager

- To understand the principles of this policy.
- Deal with any issues raised or breaches of the policy

2.3 Data Protection Officer (DPO)

- Provide advice to the organisation and its employees on data protection issues, which can include confidentiality issues, to ensure the organisation's compliance with data protection legislation.

2.4 CAB Manager

- The CAB Manager has the overall responsibility for strategic and operational management, including ensuring all policies comply with statutory and best practice guidance requirements.

4. Communication and Training Plan

This Data Protection Policy will be made available on the J: Drive and awareness cascaded through managers and supervisors. All team members are required to undertake mandatory induction training on CAS Learn. Where access to CAS Learn is not available, local arrangements should be made.

5. Lawfulness and Transparency of Processing

The UK GDPR permits organisations to use personal data where there is a clear basis for that use under Data Protection Law. The options available are set out in the UK GDPR within Article 6 (personal data) Article 9 (special category data) and Article 10 (criminal convictions data). Other conditions for processing are set out in Schedule 1 of the Data Protection Act 2018. Information about the lawful bases for processing can be accessed here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

Please consult with your DPO to identify the appropriate lawful basis for the processing of personal data by your Bureau.

When we process Special Category of Data or Criminal Conviction Data we are required to have an Appropriate Policy Document in place.

Transparency is a key principle under Data Protection Law. Whenever we collect Personal Data from clients or employees, we must be open and transparent about why we need it and how we will use it and we must signpost them to the relevant privacy notice. Grangemouth and Bo'ness CAB data processing is outlined in the Privacy Notices:

- Client Privacy Notice
- Staff Privacy Notice
- Applicant Privacy Notice

Any updates required to the Privacy Notice should be directed to the DPO for approval.

6. Data Sharing

Team Members should only share personal data outside of CAB where it is necessary. Team Members should consider the following before sharing personal data:

- Team members should refer to IT policies to ensure personal data is shared via an approved and secure method.
- Data Protection Law restricts transfer of personal data outside the United Kingdom. Seek advice from the DPO before transferring personal data to another country.
- Personal data must only be shared with approved, vetted third party service suppliers. The law requires data processing agreement to be signed and in place with all third-party suppliers.
- When sharing personal data with another Data Controller CABs must assess whether a data sharing agreement is required.

Seek advice from the DPO if you require assistance with putting in place a data processing or data sharing agreement.

In certain circumstances, Data Protection Law allows personal data to be disclosed to fulfil a legal obligation, such as to provide to law enforcement agencies. CAB should follow Network advice when considering a data request and seek advice from their DPO.

7. Data Accuracy

It is the responsibility of all team members who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary and unnecessary additional copies of data should not be made.
- Team members should take every opportunity to ensure data is updated and inaccuracies corrected. For instance, by validating customer contact information.
- Team members should keep their own personal data up to date and contact the HR Team if any updates are needed.
- All CABs are required to maintain an accurate document that outlines all of the organisations data processing activities. This is called a Record of Processing Activities ('ROPA').

8. Data Storage and Retention

All staff members are require to ensure that personal data is stored securely at all times whether stored in an electronic format or in paper format.

- When personal data is stored in paper format i.e., in reports or customer letters, it must be kept in a secure place where unauthorised people cannot have access to it.
- More information about the storage and management of electronic records can be found in our IT Policy.

It is the responsibility of the team members the ensure that Grangemouth and Bo'ness CAB must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

All staff members are required to take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our Data Retention Policy.

9. Data Protection Impact Assessments (DPIA)

A DPIA helps to identify, minimise, and document data protection risks associated with new processing activities. Grangemouth and Bo'ness CAB has a legal obligation to conduct a DPIA using the approved template when a new processing activity present a high risk, for example:

- The use of new technologies, programs, systems or processes,
- Automated processing including profiling and use of ML/AI,
- Large-scale processing of Special Category Data or Criminal Convictions Data,
- Large-scale profiling activities.

Completed DPIA's should be reviewed and signed off by our DPO.

10. Data Protection Rights

Under data protection law, individuals are entitled to certain information rights and can action these rights at any time – these include the right to withdraw consent and the right to be forgotten, as well as subject access requests (SARs). Please refer to the ICO guidance on Data Protection Rights for further information.

Individuals can make requests concerning their information rights verbally and in writing and Grangemouth and Bo'ness CAB will usually be required to respond within 1-month of receipt of a valid request (where an individual's 's identity can be verified).

Team Members should make sure they understand the different data protection rights and are confident in recognising requests. If additional training is required, this should be raised with your line manager. Any requests should be communicated to the DPO.

Where data is stored on CASTLE and action needs taken by CAS, these requests should be sent to DPO@CAS.org.uk

11. Personal Data Breaches

A personal data breach is 'the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. Practical examples include: disclosing personal data by sending an email to the wrong person; loss of a work laptop; accessing personal data only when necessary.

Grangemouth and Bo'ness CAB is required to notify the ICO of serious data breaches – one that could result in a significant risk to individuals. Failure to notify the ICO within 72 hours is a breach of the law. Failure to take action, together with the consequences of the breach itself, could expose the Bureau and wider network to investigation by the ICO, financial penalties and significant reputational damage.

If you become aware of a Personal Data Breach

1. Inform your line manager or the DPO immediately.
2. Complete the Data Breach Reporting Form at https://www.cas.org.uk/data-breach-recording-form - this is sent directly to the DPO for review.
3. Make yourself available to the DPO, your line manager and other key staff who may need you to assist in handling the Personal Data Breach.

If communicating with an individual about a breach, any communication must be sent to the network insurer ADS for review of liability. The ADS helpline can be called on 01992 636324.

12. Disciplinary

Breaches of this policy will be treated seriously by [insert CAB name] and will be dealt with in accordance with the Disciplinary Policy [enter policy name if different].

13. Related Documents and Policies

Related Policies

- Data retention policy
- Appropriate policy document