Data Protection Policy

1.1. CAB Gwynedd is fully committed to compliance with the requirements of the Data Protection Act 1998 which came into force on 1 March 2000.

1.2. The bureau will therefore follow procedures which aim to ensure that all employees and volunteers, and others who have access to any personal data held by or on behalf of the bureau, are fully aware of and abide by their duties under the Data Protection Act 1998.

1.3. CAB Gwynedd is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

2. Statement of policy

2.1. In order to operate efficiently, CAB Gwynedd has to collect and use information about people with whom it works. These may include clients; current, past and prospective employees; past and prospective volunteers; and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

2.2. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

2.3. Given the nature of the CAB service and its aims and principles, we view the lawful and correct treatment of personal information as very important to its successful operations, and to maintaining confidence between bureaux and those with whom they carry out business.

2.4. To this end, CAB Gwynedd fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 1998.

3. The Principles of Data Protection

3.1. The Act stipulates that anyone processing personal data must comply with eight Principles of good practice. These Principles are legally enforceable.

3.2. The Principles are as follows:

1. **Personal data shall be processed fairly and lawfully**
2. **Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**
3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.**
4. **Personal data shall be accurate and, where necessary, kept up to date.**

5. **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.**
6. **Personal data shall be processed in accordance with the rights of data subjects under this Act.**
7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**
8. **Personal data shall not be transferred 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.**

3.3. Petra data is stored in the UK however some limited support functions are performed remotely from India. The implications of this in terms of principle 8 of the DPA are discussed below.

3.4. The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

3.5. Personal data is defined as data relating to a living individual who can be identified from:

- that data
- 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 an 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.

3.6. Sensitive personal data is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinion
- religious or other beliefs
- trade union membership
- physical or mental health or condition
- sexual life
- criminal proceedings or convictions.

3.7. To comply with Schedule 2 and Schedule 3 of the Data Protection Act in practise, the bureau must:

a) have legitimate grounds for collecting and using the personal data;

b) not use the data in ways that have unjustified adverse effects on the individuals concerned;

c) be transparent about how the data will be used, and give individuals appropriate privacy notices when collecting their personal data;

d) handle people's personal data only in ways they would reasonably expect; and

e) make sure nothing unlawful is done with the data.

4. Handling of personal / sensitive information

4.1. CAB Gwynedd will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

4.2. These include:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information within the statutory 40 days.
- The right to prevent processing in certain circumstances.
- The right to correct, rectify, block or erase information regarded as wrong information.

4.3. In addition, we will ensure that:

- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or volunteer or a member of the public, knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.

- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

4.4. All employees and volunteers are to be made fully aware of this policy and of their duties and responsibilities, and will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. In particular they will ensure that:

- Paper files and other records or documents containing personal / sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems is protected by the use of secure passwords.
- Individual passwords are such that they are not easily compromised.

5. Use of Petra

5.1. CAB Gwynedd uses Petra to electronically record the advice given to clients.

5.2. Petra facilitates adherence to the Data Protection Act as it has a 'check box' to allow the bureau to enter the fact that consent has been obtained. This 'check box' can be updated on every contact.

5.3. The Petra servers (for data storage and application access) are hosted at the Logica Data Centre in Bridgend, South Wales. This data centre is designed specifically to host data and applications for many clients, and therefore are secured both physically and electronically. The environment, security policy and procedure for the Petra application are based on ISO 27001, as recommended by the Information Commissioner's office.

5.4. All Petra data is stored in the UK however some support staff are based in India and do access Petra data remotely to carry out support functions. This access is secured both physically and electronically and this support function has in place environmental and security policies and procedure which meet the ISO 27001 standard as recommend by the Information Commissioner's office. Under the Data Protection Act it is not permissible to transfer personal data outside of the European Economic Area (EEA) unless the territory offers an adequate level of protection for the rights and freedoms of data subjects.

5.5. The operation of a remote support function from India may involve the transfer of personal data outside of the European Economic Area. In order to meet our obligations under the 8th principle of the Data Protection Act we have sought appropriate assurance that there are adequate measures in place to safeguard the rights and freedoms of data subjects during this limited processing.

6. Implementation

6.1. CAB Gwynedd is responsible for leading and monitoring policy implementation. They will also have overall responsibility for:

- the provision of cascade data protection training for staff and volunteers within the bureau
- carrying out compliance checks to ensure adherence, throughout the bureau, with the Data Protection Act and with the Petra Acceptable Use Policy.

7. Notification to the Information Commissioner

7.1. The Information Commissioner maintains a public register of data controllers. CAB Gwynedd is registered as such.

7.2. The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

7.3. The Chief Executive will review the Data Protection Register annually, prior to notification to the Information Commissioner.

7.4. Any changes to the register must be notified to the Information Commissioner within 28 days.

8. Relationship with existing policies and supporting documentation

8.1. This policy has been formulated within the context of a range of bureau policies such as those relating to IT security, confidentiality and information assurance. Further guidance is available from the Information Commissioner's Office: ico.org.uk/for-organisations/guide-to-data-protection

Reviewed by Tal Michael, November 2016