DATED 26TH JULY 2013

DATA PROTECTION POLICY OF

JOYCE WATSON, ASSEMBLY MEMBER

REGISTRATION NUMBER Z1556334

CONTENTS

CLAUSE

1. POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of my activities I, and my office staff (and any volunteers) will collect, store and process personal information about the constituents for whom I act and others that we communicate with in order to act for and on behalf of constituents.

1.2 The types of information that we may be required to handle include details of constituents and others that we communicate with (both currently and in the past). The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

2. STATUS OF THE POLICY

2.1 This policy sets out the rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 If you consider that the policy has not been followed in respect of personal data about yourself or others you should initially raise the matter with the Office Manager.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically (for example on a computer, camera or mobile phone) or is held manually pending transfer to electronic devices. It also includes certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an expression of an opinion.

3.4 **Data controllers** are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. I am the data controller of all personal data used in my offices to enable me to fulfil my role as a member of the National Assembly for Wales.

3.5 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 **Data processors** include any person who, or organisation which, processes personal data on behalf of a data controller. An example would be the Assembly Commission's payroll provider. Employees of data controllers are excluded from this definition.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** is defined in the Act. It is information about:

- a person's racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life;

or

- the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

Sensitive personal data can only be processed if certain conditions are met. Gaining the explicit consent from the data subject is one condition that allows sensitive personal data to be handled. However, Assembly Members do not always need to obtain explicit consent to handle sensitive personal data in the course of constituency casework as legislation allows Members to handle that type of data in particular circumstances, For example, in order to take action in connection with casework requests made by constituents.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

4.1 Processed fairly and lawfully.

4.2 Processed for limited and specified purposes and in an appropriate way.

4.3 Adequate, relevant and not excessive for the purpose.

4.4 Accurate and up-to-date.

4.5 Not kept longer than is necessary for the purpose for which it was collected.

4.6 Processed in line with data subjects' rights.

4.7 Secure.

4.8 Not transferred to people or organisations situated in certain countries (including those outside of the EEA) without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that all processing is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case Joyce Watson AM), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed.

6. PROCESSING FOR LIMITED PURPOSES

6.1 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be

collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. ACCURATE DATA

8.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

9. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose for which it was collected initially. This means that data in manual files will be destroyed and electronic data erased from our systems when it is no longer required. I will retain all records in line with my retention schedule. I will keep a list of files which have been destroyed. **For example all case work will be destroyed 2 years after the file has been closed.**

10. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

(a) Request access to their personal data which is held by a data controller. This is known as a Subject Access Request;

(b) Prevent the processing of their data for direct-marketing purposes;

(c) Ask to have inaccurate data amended;

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that we hold about them must be made in writing, either in hard copy or by email. Any member of staff who receives a written request for an individual's personal data, they should forward it to Joyce Watson AM immediately.

11. DATA SECURITY

11.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor where: the processing is carried out under a contract; the contract requires the data processor to comply with obligations equivalent to those imposed on the data controller; the data processor acts only on the instructions of the data controller; and the data controller monitors adherence to the arrangements.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data. For the purposes of this policy, those terms are defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it, and 'confidential' is to be construed in a similar way.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore, for example, be stored only on IT equipment provided via the Assembly Commission and not on any individual PCs.

11.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards will be kept locked at all times if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded using a shredder with cross-cutting blades or via the arrangements put in place by the Assembly Commission. Paper documents must be retained securely pending shredding. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required. Case files closed on the Assembly Caseworker programme will be archived and deleted in line with my retention schedule.

(d) **Equipment.** Data users will ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

12. PROVIDING INFORMATION OVER THE TELEPHONE

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

(a) Check the caller's identity to make sure that information is given only to a person who is entitled to it.

(b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

(c) Refer to the Office Manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

13. MONITORING AND REVIEW OF THE POLICY

13.1 This policy is reviewed bi-annually by Joyce Watson

13.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.