City of Westminster

Committee Report

Date:	**7 July 2016**
Classification:	**For General Release**
Title:	**Data Protection Registration – Requirements for Members**
Report of:	**Head of Committee and Governance Services**
Financial Summary:	**There are no financial implications**
Report Author and Contact Details:	**Mick Steward, 020 7641 3134; msteward@westminster.gov.uk**

1. Executive Summary

1.1 As requested by the Committee at its last meeting this report sets out details of the data protection requirements for Members.

1.2 Members are asked to note that the Corporate Information Manager, who is the responsible officer and who has inputted to the paper, is not available to attend this meeting and therefore Members are asked to consider the paper and raise any issues for further discussion at the November meeting.

2. Recommendations

2.1 That the report be noted.

2.2 That the Committee indicate if any further guidance should be issued to Members or included in the Member Development Programme.

2.3 That it be noted that information about Members obligations as Data Controllers will be issued shortly.

3. Background

3.1 The Data Protection Act identifies Members as data controllers in their own right by virtue of their official role. As such all data controllers are required to maintain an entry on a public register, which identifies the nature of processing that they do. The Council undertakes this on behalf of all Members. Members are due to receive their notification of this shortly.

4. Legal Implications

4.1 As a data controller each Member is required to ensure that their handling, use, and sharing of personal data complies with the Data Protection Act 1998 [the Act].

4.2 The Act requires all data controllers comply with 8 Data Protection Principles. These are summarised below:

Principle 1: all processing must be fair and lawful

Principle 2: personal data must only be used for specified purposes

Principle 3: personal data must be adequate, relevant and not excessive

Principle 4: persona data must be kept accurate and up to date

Principle 5: personal data should not be held for longer than is necessary

Principle 6: all processing must be in accordance with the data subject's rights

Principle 7: personal data must be kept secure

Principle 8: personal data must not be transferred outside the European Economic Area

4.3 In translating the above Principles into a set of best practice actions, Members should be aware of the following key compliance requirements:

As a Member you must:

Inform constituents why you are collecting their personal data and only use it for those purposes (a Fair Processing Notice)

Remember that council information is subject to the FOI Act, and that any person has the right to request that information – including any information held on email (Right to Know)

Remember that any constituent can request their personal data– including any personal data held on email (Right of Access)

Only use personal data provided to you by the council (e.g. in the course of Committee work) for those express purposes

Keep all records secure from accidental loss and/or disclosure

As a Member you must not:

Record anything in an email that you wouldn't want seen by the person it is about (remember their Right to Know)

Use any council information - i.e. that provided to you in the course of committee work, for any other purpose than that which it was obtained for (nor in contradiction of your own Fair Processing Notice)

Share constituents' personal data with any other person or organisation, or for any purpose, unless they have given you consent to do so

Access council-held personal data for private purposes, such as when acting on behalf of your political party (Need to Know)
Retain data for longer than is necessary; instead dispose of it securely when no longer required

4.4 For more guidance Members should contact the council's Information Management Team

4.5 For further advice on the Data Protection Act 1998 contact the Information Commissioner's Office

4.6 At the time of the Council's elections the information reproduced in Appendix A was issued as part of the Members Handbook to all Members. The Committee's view is sought on whether this should be issued again as a reminder and whether for a session on Data Protection should be included in the Member Development Programme. A note on the obligations of Data Controllers will be issued shortly.

4.7 The registration of Members as Data Controllers for 2016/2017 has been completed and the certificates notifying thus will be sent shortly once received from the Information Commissioner.

5. Financial Implications

5.1 The cost of registration is £35 per annum per Member. This is met from existing resources.

6. Other Implications

6.1 There are no other implications.

If you have any questions about this report, or wish to inspect one of the background papers, please contact: Mick Steward; 7641 3134; msteward@westminster.gov.uk

Appendix A

C. Data Protection

The Data Protection Act 1998 applies to all personal data processed by or on behalf of the authority. The Act is comprised of eight principles, all of which must be met in order to demonstrate compliance. The Act applies to any organisations processing personal data, the definition of which includes any intentions or opinions expressed about the individual.

An individual has a right to be informed about what information an organisation holds on them as well as how it is being used. An organisation must satisfy itself that the applicant has a right to the information. Information about third parties is normally exempt but this is not an absolute exemption and there may be circumstances where it is disclosed. It is important that individuals understand how their information is being processed. This is achieved through an organisation's registration with the ICO and through public notices known as Fair Processing Notices.