HOUSE OF COMMONS

Advice for Members and their staff

Data Protection Act 1998
Personal information about constituents and others

IMPORTANT INFORMATION PLEASE READ

Produced for Members and their staff by the Department of Resources' Information Rights and Information Security (IRIS) Service

Sources of information and assistance

Further guidance and a copy of this booklet can be found electronically at:

- http://intranet.parliament.uk/offices-departments/iris/
- http://www.parliament.uk/site_information/foi/data_protection/commons_data_protection.cfm

Information Rights & Information Security (IRIS) Service	For advice on the contents of this booklet and the application of the Data Protection Act	020 7219 8805 iris@parliament.uk
Subject Specialist Department of Information Services	For information and research about the Data Protection Act	020 7219 3691
Clerk of the Journals Department of Chamber and Committee Services	For advice on parliamentary privilege	020 7219 3315

Information Commissioner's Office	For information and assistance on complying with the Data Protection Act	0303 123 1113 www.ico.gov.uk

Acknowledgments

Thanks are due to colleagues in the House of Commons, the Ministry of Justice and the Information Commissioner's Office, who reviewed and contributed to this guidance.

Updated March 2014

Advice for Members and their staff

Contents

Introduction

The purpose of this booklet is to assist Members of Parliament and their staff in meeting the requirements of the Data Protection Act 1998 (DPA) to look after personal information regarding constituents, staff and others in a fair and lawful manner. Parliamentary privilege does not exempt Members of Parliament from complying with the DPA with respect to constituency casework, and the requirements of the Act must therefore be observed.

A Member is the data controller for all personal data that is handled by their office and they have overall responsibility for ensuring that this is done in accordance with the DPA. Everyone who deals with personal information in a Member's office has responsibility for the personal data that they handle for the Member, and must therefore comply with the rules of the DPA.

The DPA lays down eight key principles for the handling of personal information, and outlines certain conditions that must be satisfied before personal data can be processed. These conditions are even stricter if sensitive personal data is to be processed. However, the DPA is not there to add unnecessary bureaucracy or to prevent you from doing the right thing. It is a legal framework which can benefit you and your constituents and facilitate effective and well-organised casework.

This booklet explains three key obligations:

1. Registering with the Information Commissioner's Office
2. Abiding by the data protection principles
3. Allowing people to exercise their rights.

It contains good office practice suggestions to help Members comply. This booklet also explains, at section 3.6, how the Freedom of Information Act applies to Members.

Scope and definitions

Personal data is information about an identifiable living individual. This will include any information which has been anonymised, but where the individual could still be identified by other information that the Member can access. The information may be held electronically. It also includes information in manual e.g by filing system alphabetised by peoples' names.

Sensitive personal data is information regarding an individual's racial or ethnic origin; political opinions; religions or similar beliefs; trade union membership; physical/mental health or condition; sexual life; offences committed or alleged to have been committed; proceedings for any alleged or committed offence and the resulting disposal or court sentence.

A data controller is the person who has ultimate responsibility for any personal data and who determines the purposes for which personal data is to be processed. In a Member's office, this will always be the Member.

A data processor is any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

The Information Commissioner's Office (ICO) is the UK's independent public body set up to protect personal information and enforce the DPA. The Information Commissioner has powers to investigate complaints; issue Notices on data controllers; enter and inspect premises and information; fine† for non-compliance.

Data protection principles are eight rules which must be complied with whenever personal data is handled.

Processing covers almost any action that can be carried out with personal data, including receiving, recording, holding, changing, retrieving, disclosing, erasing and destroying.

Whilst reference is largely made to constituents throughout this booklet, the guidance applies to personal data held about anyone.

†*Refer to the ICO for up-to-date details regarding powers to fine and prosecute.*

Section 1: Register with the Information Commissioner

Members of Parliament must register with the Information Commissioner's Office (ICO) and renew their registration annually if they use Information Technology to process personal data, e.g. if your office uses computers. A Member is the data controller for all personal data handled by their own office. This will include information on many individuals, and not just information on constituents who voted for them. Therefore, each Member must register individually even if their local party organisation is already registered. The process of registering is often referred to as notification and a copy of a Member's notification, excluding the mandatory security statement, will be made available by the ICO on a public register.

Details on how to notify, including a notification handbook which contains answers to commonly asked questions; an explanation of the notification life cycle; and a guide on how to complete the notification form are available on the ICO website.

The ICO has a template notification form tailored for Members of Parliament. You can add, amend or delete any of the categories included in the template, according to the nature of personal data processing that you undertake. The template form will be sent to you if you call or write to the ICO asking for a notification form. If you wish to find the form online, go to the notification pages on the ICO's website and select the following options to open the appropriate template form: 'Religious/ Political/Charitable' on page DP4 (Template Categories) and then 'N862 MP – Member of Parliament' on page DP5.

There is an option to tick a box indicating whether you are a public authority for the purpose of the Freedom of Information Act 2000 or a Scottish public authority for the purpose of the Freedom of Information (Scotland) Act 2002. Members of Parliament are not public authorities

for these purposes and there is therefore no need for you to tick this box or to pay the associated higher notification fee.

Once the notification form has been completed, it needs to be signed and dated and then posted to the ICO together with a notification fee of £35. The form cannot be submitted online, by fax or by email and it is advisable to keep a copy of your completed notification form. The fee can currently be claimed against the Administrative and Office Expenditure. Details of how to pay by cheque or BACS and a link to a form for paying by direct debit is on the ICO website, notification page DP9.

The ICO Notification Helpline

01625 545 740 open 9-5 Mon-Fri

The ICO notification handbook:

http://www.ico.gov.uk/upload/documents/notifications_handbook_html/index.html (interactive)
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/notification_handbook_final.pdf (printable)

Information Commissioner's Office
PO Box 66
Wilmslow
Cheshire
SK9 5AX

Section 2: The data protection principles

Members and their staff must follow the eight principles which set out the minimum requirements under the Data Protection Act 1998.

The data protection principles (refer to the Act for exact wording)

1. Personal data must be processed fairly and lawfully and shall not be processed unless certain conditions are satisfied

2. Personal data must be obtained and processed for specific and lawful purposes. It must also only be processed for purposes which are compatible with those for which it was obtained

3. Personal data must be adequate, relevant and not excessive for the purposes it is being processed for

4. Personal data must be accurate and (where necessary) up to date

5. Personal data must not be kept for longer than is necessary

6. Personal data shall be processed in accordance with the rights of data subjects

7. Personal data shall be protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage

8. Personal data shall not be transferred outside the European Economic Area without adequate protection for the rights and freedoms of data subjects in relation to personal data

Remember, 'processing' covers almost anything you might want to do with information: obtaining it, using it, sorting it, passing it on, destroying it, and even simply holding it.

2.1 Principle one: fair and lawful

2.1.1 The first principle is the most complex and, arguably, the most significant principle.

2.1.2 The obligation to handle personal data 'fairly' means that before you do anything with it, you must be reasonably sure that the person concerned knows:

- who is legally responsible for the use made of the information. (i.e. the Member as data controller)
- why you are asking for the information (if that is what you are doing)
- what the information will be used for and
- any other relevant information such as who will be seeing it, and how long it will be kept

GOOD PRACTICE TIP: Use privacy notices whenever you collect personal information about people and put a privacy notice on your website. See section 5.5 for guidance.

2.1.3 In most cases if a constituent asks a Member to help with a problem they expect the Member to store the information they send and sometimes to copy it to another person or organisation who might be able to help. If so, you do not need to write to the person especially to give them this information. But constituents will not always know this. Use your discretion, and if you think a constituent may be surprised about what you plan to do with information about them, then explain your plans to them.

2.1.4 'Lawfully' means that the handling of the information must not infringe the laws of this country. Of particular relevance is the common law duty to protect confidential information.

2.1.5 The Act requires that one 'condition' (from a list) must be met whenever personal data is processed. It **also** requires that a further 'condition' (from another list) must be met if 'sensitive personal data' is to be processed (see p3 for a definition). See 'Section 4: When to get consent' for an explanation of what a Member needs to be aware of in relation to these conditions when handling constituency casework.

2.1.6 In relation to sensitive personal data which is held about your own staff, there is a condition which allows personal information to be processed if it is legally required for employment purposes.

2.2 Principle two: specified, lawful and compatible purposes

2.2.1 You must be clear and open about the purpose for which personal data is obtained and held. You must not then use this data for a different purpose unless it is compatible with the original purpose and it is lawful to do so.

2.2.2 A constituent contacting their Member about an issue will not necessarily want their details used for any purpose other than that stated in their letter. It is unlikely to be lawful to use this information for other purposes, for example political canvassing, campaigning or promotion of a political party.

2.2.3 Seek consent if you wish to use personal data for a purpose which was not specified or understood when you collected the information.

GOOD PRACTICE TIP: Ensure that any information you obtain, hold, use or pass on is relevant to the specific issue for which you obtained it, and that issue only. Effectively, this means 'pigeon holing' constituents' information and not using that information for any other purposes. Information from constituency casework should not be used for political campaigning without permission. Refer to section 5.6

2.3 Principle three: adequate, relevant and not excessive

2.3.1 Make sure that you do not ask for or record too much or too little information for the purpose for which it is required. Do not obtain or keep information in case it might be useful, or because it could be useful for a different purpose that you have in mind.

2.3.2 Only record relevant personal information, and do so in a manner which you would be happy to show to the person who is the subject of that information.

2.3.3 When contacting other organisations to represent an individual, consider how much information it is necessary to give to the other organisation in order for them to address the needs of your constituent. It may be possible to withhold some of the detail and still successfully represent your constituent.

GOOD PRACTICE TIP: Ensure that forms and other media in which you obtain information from individuals do not ask for more information than is necessary. When filing casework, consider whether you need to keep all the information you are holding. Delete or shred any irrelevant information which you do not need to keep.

2.4 Principle 4: accurate and up to date

2.4.1 You must make sure that any personal information you use is accurate. This is particularly important if it has been obtained from another person or organisation rather than directly from the subject of the information. Take particular care with constituents' contact details, to ensure that correspondence is not sent to the wrong address.

2.4.2 Getting casework details wrong could cause distress or problems for a constituent or embarrassment for a Member. Individuals have a right to correct inaccurate information (see section 3.4). Care should be taken in ensuring accuracy when following up any cases which deal with information about individuals, particularly where consent has been given to do so in public.

GOOD PRACTICE TIP: Implement a system of auditing the personal information which you receive or hold to ensure that it is accurate and up to date. For example, if a dormant case becomes live again check that the facts are up to date with the individual concerned.

2.5 Principle 5: not kept for longer than necessary

2.5.1 The Data Protection Act does not outline time periods for how long records should be kept for. Identify the different types of record you hold, such as constituency case files, employment records, or contact details, and consider how long would be reasonable to keep each type of record. Appropriate periods are determined by other laws and by accepted best practice. See section 5.3 and 6.4 for guidance.

2.5.2 The benefits of this principle can be felt in a number of areas. Destroying information when it is no longer required reduces physical and electronic storage space; removes the need for it to be updated; and saves time when handling requests for access to information.

2.5.3 Keep a log of what is destroyed, why and when.

GOOD PRACTICE TIP: Introduce clear office procedures to ensure that destruction of old records is not neglected. See section 5.3 and 6.4.

2.6 Principle 6: the rights of data subjects

2.6.1 The Data Protection Act gives people various rights, including the right to access information held on them. These rights are identified in section 3, with guidance on how to handle requests.

GOOD PRACTICE TIP: Draw up procedures for dealing with requests from individuals to exercise their rights. Train all staff to be able to spot and handle such requests. See sections 3.5 and 3.7 for assistance.

2.7 Principle 7: protected by appropriate security

2.7.1 Losses of personal or sensitive data by various bodies have highlighted the importance of this principle. The losses have emphasised the value of putting in place appropriate measures to ensure that

information is secure. They have also drawn attention to the potential consequences of failing to take appropriate steps to guard against loss of data.

2.7.2 Keep personal information secure and introduce office practices to ensure that security measures are followed. See section 5.2 for guidance. Take particular care when sharing information or sending it off-site.

2.7.3 Ensure that appropriate provisions are put in place for anyone who can access personal data, including staff, volunteers and third party suppliers. Formalise these provisions in contracts and confidentiality agreements. See section 5.1 and 5.2 for guidance.

2.7.4 Use your discretion to decide what security measures to apply in any given circumstance, as these will vary according to the nature of the data concerned.

0

GOOD PRACTICE TIP: Audit the security of your office and information systems. A contribution towards extra security measures for the office may be obtainable through allowances. See section 5.2.

2.8 Principle 8: not transferred outside the EEA

2.8.1 If you need to send personal information across national borders, you must be assured that the other organisation/country in question has both adequate legal protection for handling personal information and a legacy of solid practices. You do not want your fair and lawful processing procedures to be compromised by deficiencies in other countries.

2.8.2 Information on a website is considered to be transferred outside of the EEA only if it is viewed, or intended to be viewed, by someone who is not resident in the EEA.

GOOD PRACTICE TIP: If you put personal information on to your website be sure that the individuals concerned do not mind their information being used in this way.

Section 3: Individuals' rights and access to information

Individuals have a number of rights under the Data Protection Act including, but not limited to, the right to access their own personal information. This section outlines the rights of individuals which are most likely to be relevant in a Member's office and suggests at 3.7 a process for handling subject access requests. It also explains at 3.6 the position of Members in relation to Freedom of Information. Further detail can be found in the legal guidance on the Data Protection Act on the Information Commissioner's website.
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

3.1 The right to prevent handling which causes damage and distress

3.1.1 If someone believes that you are using information about them in a way which causes them substantial and unwarranted damage or substantial and unwarranted damage and distress, they have the right to send you a notice telling you to stop within a reasonable time. (NB: This right is not available in all cases. For example, it is not available if the person concerned has given valid consent to use the information about them in this way.)

3.1.2 If one of these notices is received, the first step is to check (by consulting the legal guidance on the Information Commissioner's website) whether the person has the right to issue a notice of this sort. If they do have the right, a response must be given to the individual within 21 days either indicating an agreement to comply fully or giving an explanation as to why the request was unjustified.

3.2 The right to correct inaccurate information

3.2.1 People can apply to the courts for an order requiring inaccurate information about them to be corrected, blocked, erased or destroyed. In some cases if the inaccurate information has been passed to a third party, the courts may order them to be contacted to correct this.

GOOD PRACTICE TIP: If an individual complains that information which you hold or use about them is inaccurate or misleading, be prepared to change, update or erase that information if it is appropriate to do so - even before he/she makes a formal challenge.

3.2.2 You are perhaps unlikely to have to deal with a court order of this sort. However, the Information Commissioner has wide-ranging powers and can investigate if someone complains to him.

3.3 The right to compensation

3.3.1 People who think they have suffered damage can claim compensation if provisions of the Data Protection Act have not been followed. They have to apply to the courts for this. The courts can order compensation for any damage suffered. Compensation can also cover distress.

3.4 The right to prevent processing for direct marketing

3.4.1 Direct marketing refers to the communication of information to named individuals by post, telephone call, text message, email, fax or any other medium. It includes promoting the aims and ideals of a political party, as may be included in correspondence sent directly to named constituents through a Member's newsletter or update.

3.4.3 The Information Commissioner has produced guidance on the promotion of a political party with respect to the provisions of the Data Protection Act and the Privacy and Electronic Communications Regulations 2003 which can be found at www.ico.gov.uk.

3.4.4 People have the right to give notice in writing to prevent processing of their personal data for the purposes of direct marketing or advertising. They may also register their desire not to receive direct marketing through the Telephone, Fax or Mail Preference Services.

Unsolicited marketing should not be directed at anyone who has registered for one of these services. Further information can be found at www.tpsonline.org.uk.

GOOD PRACTICE TIP: Make sure you have an individual's consent before you send them material promoting political aims or activities. Ensure that you include clear instructions on how to opt out of receiving this information in all such materials.

3.5 Individuals' right to access information about themselves

3.5.1 Under the Data Protection Act, individuals have a right to ask:

- whether you are processing their personal data
- for a description of their personal data and the purpose it is held
- for a description of who (people/organisations) might see their personal data
- for a copy of the information

3.5.2 If you receive a request from an individual for access to personal information that you hold about them, you must consider this request under the Data Protection Act. You must respond even if the request does not refer to the Data Protection Act, or if it incorrectly refers to the Freedom of Information Act. (refer to section 3.6)

3.5.3 Requests must be made in writing indicating what information is sought. You are entitled to charge up to £10 for handling these requests, but we recommend Members do not charge this fee.

3.5.4 Requests must be responded to within 40 calendar days. Guidance on handling requests is outlined under section 3.7 below.

3.5.5 If you receive a request from someone on behalf of a child or another adult then you will need to satisfy yourself that they have authority to do this.

3.6 Freedom of Information

3.6.1 If you receive a request under the Freedom of Information Act 2000 (FOIA) for access to any other information, you are not obliged to provide it. The FOIA only applies to public authorities, and Members of Parliament are not public authorities for the purposes of the FOIA. You can choose to provide information voluntarily if you feel it is reasonable and appropriate to do so. You may also refer the requester to a public authority that does hold the information. See section 7.14 for a template response letter.

3.6.2 The House of Commons is a public authority for the purposes of the FOIA. This applies to information that it holds in its own right about Members. However, it does not apply to information held by Members regarding their Parliamentary and constituency capacities which is stored physically or electronically at the House of Commons.

3.6.3 For further information about the FOIA and its application to Members, please refer to our intranet page which contains links to the Information Services research papers and standard notes: http://intranet.parliament.uk/legal-advice/foi.

3.7 Handling requests for access to personal data

3.7.1 If you receive a request for access to an individual's own personal data, you must check that the following three points are satisfied. If they are not, you must immediately tell the requester what you need to satisfy these points.

- Make sure the request is in writing. If the information has been asked for verbally, ask the requester to put it in writing. Assist them in doing this if necessary.
- Make sure you are confident about the identity of the requester. If you are not, ask them for proof of identity.
- Make sure you understand what the applicant is looking for. If you are not sure, ask them to be clearer and to give you any information they can to help you find it. You can save a lot of time if you know exactly what the individual is looking for

3.7.2 When these three points are satisfied, start the clock. You must respond to the request promptly and always within a maximum 40 calendar days.

3.7.3 Conduct a search of your paper and electronic records for the requested information.

3.7.4 Check the information you have collated to see if there is any:

- information about someone else
- correspondence from another person
- information given in confidence by e.g. a legal adviser

If so, consider whether it would be appropriate to share this information. You may need to seek consent from the third parties concerned to determine this. For example, if there is information about the requester's health, you may need to consult a health professional regarding its disclosure. Alternatively, it may be appropriate to black out information to remove information that should not be seen or to prevent a third party from being identified.

3.7.5 Check for any other information which you do not think the individual should see. If there is, consult the Information Commissioner's legal guidance, refer to the exemptions of the Data Protection Act to see if any apply, or seek legal advice on whether it should be disclosed. Information can only be withheld if an exemption applies.

3.7.6 Arrange to send all information that can be disclosed to the person who has requested it. Alternatively, you can arrange for the requester to come and view the file if it would involve 'disproportionate effort' to send them the information, or if the requester is happy to do so.

3.7.7 Do not destroy any requested information once you have received a request, as this could be a criminal offence.

Section 4: When to get consent

4.1 Obtaining consent to handle constituency casework

4.1.1 The first data protection principle requires certain conditions to be satisfied before personal data can be processed (see section 2.1). One condition, from a list, has to be satisfied whenever standard personal data is processed. An additional condition, from a separate list, has to be satisfied if sensitive personal data is processed.

4.1.2 There is sometimes confusion about whether or not it is necessary to get consent to satisfy these conditions. This section explains the requirements for a Member when handling personal data in the course of casework. Further guidance from the Information Commissioner can be found on the parliamentary intranet.

4.2 Consent for Members to handle personal data

4.2.1 Consent from the subject of personal data is one condition that can allow a Member to handle personal data. It is often implied when a constituent contacts a Member and asks for assistance that they want their Member to use their information, as appropriate, in order to assist them in the issue they have contacted the Member about. Where this is clearly the case, a Member can handle the case without asking the constituent to specify their consent.

4.2.2 If you think a constituent may be surprised if they knew what you were planning to do with their information, or if it is not clear what action they expect you to take, then you should discuss this with them.

GOOD PRACTICE TIP: Explain to constituents clearly what you intend to do with their information whenever opportunity offers.

4.3 Consent for Members to handle sensitive personal data

4.3.1 Explicit consent from the subject of personal data is one condition

that allows sensitive personal data to be handled (see p3 for a definition of sensitive personal data).

4.3.2 Members, however, do not always need to seek explicit consent to handle sensitive personal data in the course of constituency casework, as there is another condition (the 'Elected Representatives condition' [1]) which allows Members to handle sensitive personal data in the circumstances outlined below.

4.4 Handling sensitive personal data about a constituent when the constituent has contacted the Member

4.4.1 The 'Elected Representatives condition' allows Members to handle sensitive personal data in order to take action in connection with requests from individuals, without having to obtain explicit, written consent from that individual. Again, if the wishes of the constituent are at all unclear, you should discuss this with them.

4.5 Handling information about a constituent when the constituent has not contacted the Member

4.5.1 If you are dealing with personal information which is given to you by someone other than the subject of the information, you may need to satisfy yourself that it is acceptable to hold or use that information. For example, sometimes someone may send you information about a friend or relative and ask you to act for them. In this case you will need to use your judgement when you decide what to do.

4.5.2 As a general principle, if at all possible you should ascertain the wishes of the person concerned. See section 5.10 for further guidance.

4.5.3 If it is not possible or appropriate to seek the views of the constituent, the 'Elected Representatives condition' allows you to act without that person's consent in certain circumstances:

[1] Contained in the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002

- If the constituent cannot give, or be expected to give, consent.

  For example, if a constituent has been charged with an offence while on holiday abroad. Their family might ask an elected representative to intervene urgently to help them to get home – but it might be difficult to gain their consent, particularly if they have no access to a telephone.

- Seeking consent would prejudice the action needed to be taken.

  For example, if the matter relates to a complaint that a constituent is committing benefit fraud.

- The action is necessary in the interests of another individual, and consent has been unreasonably withheld.

  For example, if an individual requires assistance in caring for their parent as the burden of caring is putting the individual at risk of ill-health, and that parent refuses to give consent.

4.6 Consent for other organisations to release personal data to a Member for the purpose of casework

4.6.1 The 'Elected Representatives condition' allows third parties (such as Government Departments or local authorities) to disclose sensitive personal data to a Member who is acting at the request of individuals where the data are relevant to the Member's request and the disclosure is necessary to respond to the Member's request.

4.6.2 The 'Elected Representatives condition' is permissive; it does not compel third parties to disclose information to a Member.

4.6.3 Third parties may ask you to demonstrate that you are acting on your constituent's behalf in order to reassure themselves that they are complying with the Act by giving information to you. See section 5.12 for guidance.

Section 5: Office practices

This section suggests best practice which a Member's office can adopt to help comply with the data protection principles. These are only suggestions, and should be varied or added to as necessary.

5.1 Responsibilities, guidance and training

5.1.1 Require everyone working in the office to sign up to their data protection and confidentiality responsibilities. For staff, these can be defined in their contract. For volunteers, interns, agency and contract staff, these can be defined in a confidentiality agreement, a template for which can be found in section 7.1.

5.1.2 Train staff and volunteers so that they know what they can do with personal data, when they can share it and how to protect it. For central courses available for Members' staff see www.w4mp.org.

5.1.3 Develop office instructions covering data protection and confidentiality to be given to all staff and volunteers.

5.1.4 Nominate a data protection officer. Although the Member cannot delegate their responsibilities as the data controller, it is a good idea to ask someone to take the lead in being aware of and addressing data protection issues on a day-to-day basis.

5.2 Information Security

5.2.1 Make constituency and parliamentary offices secure by:

- Locking up whenever the office is vacant
- Never leaving visitors unattended
- Ensuring computer screens cannot be seen by passers-by
- Implementing secure working at home guidelines
- Using confidentiality agreements for staff and volunteers
- Training staff to know when they can pass information to others and to check with constituents when this is unclear

- Taking particular care in shared buildings
- Using the central security budget for additional security measures e.g. locks or alarms. A report from your local police crime prevention officer is required.
  See http://intranet.parliament.uk/finances/allowances/security

5.2.2 Protect information held electronically by:

- Using access controls to restrict access to information
- Password protecting files saved on portable storage devices
- Encrypting laptops and memory sticks
- Keeping the minimum information on portable storage devices
- Not sharing passwords
- Regularly backing up documents
- Wiping computers and other electronic storage devices when they are no longer needed
- Making use of further guidance on ICT security available at: http://intranet.parliament.uk/pict/services/security

5.2.3 Protect paper records by:

- Locking away paper files when they are not in use
- Shredding all confidential waste
- Not leaving confidential waste sacks lying around
- Only transport minimum information away from the office
- Lock information in briefcases or seal in envelopes marked with a return address when transporting away from the office

5.2.4 Protect information held by third party suppliers by:

- Obliging them to meet data protection requirements regarding security in their contracts
- Building in measures to check that third party suppliers are meeting these security requirements.

5.3 Disposing of records

5.3.1 Introduce a clear policy on how long all records should be retained, including constituency case files and staff records, in keeping with legal requirements and best practice.

5.3.2 There is no specific period defined by law regarding how long constituency case files should be kept, as long as they are not kept for longer than necessary for the purpose for which they are held. The purpose for holding a closed case file will finish when a reasonable period has passed from the closure date to allow for any need for the case to be reopened. The information may then be destroyed. This 'reasonable period' can be determined locally, but we usually suggest two years or the length of a Parliament as a minimum. Some more detailed files, e.g. CSA, Benefits Agency, Prisons, may need to be kept longer.

5.3.3 See section 6.4 for managing records when a Member leaves their seat.

5.3.4 When deciding how long other records should be kept, it may assist you to consult the Authorised Records Disposal Practice which has been developed for use by staff of the House of Commons and the House of Lords. It is not aimed at or designed for Members. However, it may give you an indication of the legal or best practice periods that may be relevant for different types of data.
http://pdvnsco.parliament.uk/archives/recordsmanagement/default.htm

5.3.5 Always ensure that records are destroyed securely.

5.3.6 Keep a log of records that have been destroyed.

5.4 Parliamentary privilege and Members' speeches

5.4.1 Proceedings in the House, in its Committees, and in Westminster Hall, are protected by parliamentary privilege. This means that what Members say in the course of proceedings cannot be questioned in the courts.

5.4.2 Nevertheless, Members ought to do all they can to ensure that any personal data disclosed under the protection of parliamentary privilege is accurate, relevant and appropriate.

5.5 Telling people what you do with their information

5.5.1 Be open and clear about what you do with personal information that you collect and hold by using privacy notices on forms and questionnaires, petitions, in the office, at advice surgeries and in correspondence. Doing this should reassure constituents that they can trust you with their personal data. See section 2.1.2 for what a privacy notice legally has to state.

5.5.2 Publish a clear and informative privacy notice on your website to help people to understand what will be done with their information. If you collect statistics on website activity using cookies (text files which collect standard internet log information and visitor behaviour), then you must refer to this in your privacy notice.

5.5.3 If you make use of Closed Circuit Television, refer to the Information Commissioner's Code of Practice on CCTV for guidance http://www.ico.gov.uk/upload/documents/cctv_code_of_practice_html/index.html

5.5.4 Example privacy notices can be found in section 7.2-7.5 and the Information Commissioner's privacy notice guide can be found on the ICO website www.ico.gov.uk.

5.6 Mailing lists, marketing and the electoral roll

5.6.1 Do not add a constituent's contact details to a mailing list unless you are sure that they wish you to do so. A constituent contacting you about an incinerator by their home will not necessarily want to be added to a mailing list about a Member's activities with respect to the environment or waste management. See section 3.4 for further information on the law in relation to mailing lists and marketing.

5.6.3 Whenever you send marketing material directly to named constituents, include details on how they may opt out of receiving such material.

5.6.4 Take care if you are considering using the electoral roll to contact constituents. The edited electoral roll contains the names of those individuals who are willing for their contact details to be bought and used for any purpose. The full electoral roll, which a Member of Parliament may access for their constituency by virtue of their office, lists everyone who is entitled to vote. The full electoral roll may only be used by a Member for purposes in connection with their office or for electoral purposes. It is a criminal offence to use the full electoral roll for any other purpose.

5.7 Interviews and advice surgeries

5.7.1 Use a standardised form for collecting information which contains a space for the constituent to sign their agreement. An example form can be found in section 7.8.

5.7.2 Keep handwritten notes factual and succinct and write down significant quotes precisely. Do not record your own speculative or subjective impressions of the constituent or their issue.

5.8 Telephone enquiries

5.8.1 Be careful if someone asks for personal information over the phone and do not share personal data unless you are sure of whom you are talking to. You can check someone's identity by asking them to answer a question that you can check against something you already hold. Or you could ask them to bring proof of identity to the office.

5.8.2 You can deal with casework requests received via telephone enquiries. It is good practice to take notes and treat these as carefully as other case file documentation.

5.9 Correspondence with constituents

5.9.1 If a constituent has contacted you and it is unclear what action they want to be taken as a result from that contact, check with them so that you are clear. Do not use their personal data for any other purpose.

5.9.2 Assume that information received from or about your constituents should be treated confidentially unless you are told otherwise.

5.9.3 When you first reply to a constituent who has asked you for assistance, include a standard paragraph which acknowledges that you will handle the personal data they have given you as necessary to pursue their issue, and that you will treat it in accordance with the Data Protection Act. See section 7.3 for a template.

5.10 Requests to take action relating to a constituent

5.10.1 If you are asked to take action in relation to one of your constituents by someone else, you should ascertain whether it is possible or appropriate to obtain the consent of the constituent to be represented.

5.10.2 If it is possible and appropriate, you will need a record of the constituent's wishes. You could ask the person who has contacted you to provide you with this record if you are confident that the evidence they provide will be valid. The record of the constituent's wishes should be made in writing where possible. See section 7.10 for a template.

5.10.3 If it is not possible or appropriate, you may be able to take action without consulting the constituent. The circumstances where this may be appropriate are outlined in section 4.5.

5.11 Requests to act on behalf of non-constituents

5.11.1 There is a strict parliamentary protocol that Members of Parliament do not seek to intervene in matters raised by the constituents of other Members.

5.11.2 If you are asked to take action in relation to someone who is not your constituent, do not automatically forward the request to the appropriate Member, as this may breach the Data Protection Act.

5.11.3 You should inform the person who has contacted you that you are unable to assist, and direct them to the correct person to write to. Whilst this may seem long-winded, there may be a reason why the individual would not want their own Member to be involved. See section 7.12 for a template.

5.12 Contacting others about constituency casework

5.12.1 Section 4.6 explains that other agencies are empowered, but not compelled, to share relevant personal data with Members where this is required in the course of constituency casework.

5.12.2 When discussing casework orally with other agencies, make a point of referring to the requirements of data protection legislation and the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002, particularly where constituents' sensitive personal information is involved. Be aware that such agencies are also acting within the provisions of the Act and may want reassuring that you are acting on behalf of the person concerned.

5.12.3 When contacting another agency or Government Department with details of a constituency case, you may find it helpful to include a standard reference stating that you are doing so under the provisions of the Data Protection Act. See section 7.11 for a template.

5.12.4 You may find it saves time when seeking information about your constituent from other agencies to provide a form signed by them as evidence that they asked you to take action on their behalf. See section 7.13 for a template.

5.12.5 If you need to pursue casework in a country outside the European Economic Area, do not transfer personal data unless that country ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

5.13 Information about staff and volunteers

5.13.1 A Member is legally responsible for the handling of personal information about their staff and volunteers as well as their constituents. The data protection principles must be complied with, including keeping the information secure, communicating what will be done with the information, keeping the information accurate and up to date, and allowing staff to exercise their right of access.

5.13.2 The Department of Human Resources and change in the House of Commons provides personnel advice to Members. This means that they hold some information about Members' staff on the Members behalf.

5.13.3 Staff and volunteers can apply to the Department of Human Resources and Change to see the information which it holds about them. Information will be disclosed to them only if it is fair and lawful to do so. Information will be considered for disclosure in line with the right of access under the Data Protection Act and Members will be consulted where relevant.

Section 6: Handling personal data during dissolution and when a Member leaves the House

6.1 Handling personal data when Parliament is dissolved

6.1.1 Members may continue to handle casework whilst Parliament is dissolved for all individuals who are content for this to happen. If there is any doubt, consent should be sought.

6.2 Members not standing or not returned after an election

6.2.1 Members who are not standing for re-election should begin to review their records, following the guidance below, as soon as possible having decided not to stand. A template notice which can be included in correspondence to constituents about what will happen to their casework and to offer them an opportunity to express their wishes can be found in section 7.15.

6.2.2 Former Members who are not returned after a general election should review their records, following the guidance below.

6.2.3 Any records belonging to a former Member which are left in their offices on the parliamentary estate or on computer equipment returned to PICT will be securely destroyed. Refer to dissolution guidance for precise arrangements and the timing of any such destruction.

6.2.4 For those who cease to be Members of Parliament after an election, the authority to handle sensitive personal data under the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order lasts until the end of the fourth day after the election. Section 4.3 explains what this Order means.

6.3 Handling personal data if a Member dies or leaves mid-term

6.3.1 Constituency casework may be handled until the end of the fourth day after a new Member is elected for all constituents who are content for this to happen. If there is any doubt, consent should be sought.

6.3.2 The records held should be reviewed in line with the guidance below.

6.4 Reviewing records

6.4.1 A former Member will continue to be the data controller for all paper and electronic records that they hold and they must therefore be sure that anything they do with their records is in line with the expectations of the individuals concerned. For example, constituency casework records should not normally be passed on to a new Member or to a history centre/county archive unless the constituent is happy for this to happen.

6.4.2 Records relating to closed cases which are not likely to be reopened should usually be securely destroyed.

6.4.2 Live cases, and closed cases which are likely to be reopened, should be assessed on a case-by-case basis, considering the expectations of the individuals and consulting with them where their views are not clear. Options that could be offered to constituents include

- Destroying the case-file
- Passing the case-file to the new Member
- Passing the case-file to the constituent themselves

A template form for a constituent to indicate their preference can be found in section 7.16

6.4.3 If a case-file is to be passed on, either to the new Member or to the constituent, it should be checked first to ensure that it does not contain any confidential information which either party should not see. The guidance under sections 3.7.4-5 may assist.

6.4.4 Explicit consent from the constituent is always needed to pass on cases containing sensitive personal data to a new Member.

6.4.5 Notification to the Information Commissioner should be reviewed.

6.5 New Members

6.5.1 It is understood that Government Departments are advised not to forward information about existing cases to a new Member without the constituent's explicit permission.

Section 7: Templates

This section contains a number of templates which should be adapted as relevant to make them appropriate for the purpose for which they are to be used.

7.1 Confidentiality agreement for signature by volunteers, interns, agency and contract staff etc

I undertake to preserve the confidentiality of any information which may be acquired by me in the course of my activities supporting the office of _____ MP. I understand that while supporting the Members' office I may have access to personal information about others. I undertake to act only on the instructions of the Member when handling this information, and to observe the data protection principles as set out in the Data Protection Act 1998. I undertake not to publish or otherwise disclose any such information to any third party, or to use it for any purpose, unless authorised by the Member. I expressly acknowledge that these undertakings will continue to have effect after my activities in the Member's office have ceased.

Signed _____ Date _____

7.2 Website privacy policy

Privacy policy for (name of Member)

Any personal information that you give to me will be handled confidentially by me, the staff and volunteers in my office, in line with the requirements of the Data Protection Act 1998. If you would like information about the Data Protection Act 1998, this can be obtained from the Information Commissioner's Office through their website www.ico.gov.uk or advice line 08456 306 060.

What information do we collect about you?

My office collects personal information that is supplied to me in my role as a Member of Parliament. It includes information supplied by my constituents and others in relation to matters which I have been asked to pursue in the interests of individuals and groups who live in my constituency such as:

- details of specific cases
- information provided by signatories on petitions

(cont…)

(privacy notice cont…)

- responses to questionnaires and
- contact details for the purpose of communicating news and updates

(Insert if applicable: I also collect information on use of my website using cookies.)

How will we use the information about you?

If you ask me to pursue a matter on your behalf, I will use your information in order to pursue the matter you have raised with me. My staff and volunteers will normally see this information to find help and advice for you. Your personal and sensitive personal information may be passed to other agencies (such as the Department for Work and Pensions, the CSA, the local Housing Department) if I believe this to be necessary to pursue the matter you have raised with me. Your information may also be passed on to the House of Commons Information Office to obtain further information about your case. I intend that only the minimum possible personal information will be shared with other agencies, as necessary to further your cause.

If you give me personal information about someone other than yourself, I may need to check the facts with that other person. If you ask me to take action on behalf of a friend or relative I may need to contact that person to confirm that they are happy for me to act on their behalf. If you feel it would not be appropriate for me to contact the other person, you should discuss this with me when you give me their information.

Constituency news and events

I would like to send you information about constituency news and events, but I will not use your contact details to do this unless you have said that you would like to be sent this information. If you have said that you would like this information, but later change your mind, you have a right at any time to let us know if you no longer wish to be sent this information. If you wish to receive or stop receiving this information, please contact my office.

Access to your information and correction

If you wish to see any information that I hold about you, if you want me to update or correct any personal information that I hold about you, or if you have any queries regarding personal data that I hold about you, please contact my office.

[Cookies

If you collect statistics on website activity using cookies (text files which collect standard internet log information and visitor behaviour), then you must refer to this in your privacy notice. It is suggested that you also inform users that they are able to disable cookies, but that some features of the website may not function as a result, if this is the case.]

(cont…)

(privacy notice cont…)

Other websites

This privacy notice only applies to information on my website and does not apply to information contained on other websites that are linked from this one.

Changes to our privacy policy

This privacy policy was last updated on *(insert date).*

How to contact us?

Please contact my office if you have any queries regarding this privacy policy or how my office handles your information. *(insert contact details)*

7.3 Data privacy notice for forms and questionnaires

How we use your information

The information you have provided on this form will be used by (*insert MP name*) who will be the data controller for this data, for the purposes of (*insert description of what the information will be used for*).

The information will be processed by constituency office staff but may/will have to be passed to others, for example (*insert description of who else might see it and why. You may also like to indicate how long it will be kept for*).

Your information will be processed in accordance with the provisions of the Data Protection Act 1998. If you have any questions or concerns about how your information will be processed or about your rights under the Act please contact (*insert contact details*).

7.4 Consent to use personal data for constituency news updates

Constituency news and events

We would also like to use your information to let you know about constituency news and events that may be of interest to you. If you would like to receive this information please tick the box below. If you do not wish to receive any information you do not have to do anything.

Yes, I would like to receive information about constituency news and events:

By post [ ] By email [ ] By telephone [ ] By SMS [ ]

You can contact us at any time if you change your mind and no longer wish to receive information from us.

7.5 Data privacy notice for petitions

This petition will be given by _(*insert MP name*)_ to _(*insert organisation name*)_ to demonstrate public support for _(*insert issue being subscribed to*)_. Please do not sign the petition if you do not want your details to be passed on to _(*insert organisation name*)_.

_(*insert MP name*)_would like to use the details you provide to keep you up to date about the campaign. If you are happy to be contacted in this way please tick the 'tick here to receive campaign updates' box next to your signature above. Your details will not be used for any other purpose.

7.6 Opt-out text to include in newsletters and marketing material

If you no longer wish to receive _(*insert description e.g. this newsletter*)_, please inform me on _(*insert contact details*)_

7.7 Record of a constituent's wishes

I confirm that it is my wish for you to pursue the matters I bring to you. In order to do so you may use all information I have provided about me, whether written or spoken, and including sensitive personal information. I understand that you will do so in line with the requirements of the Data Protection Act 1998.

Signed: _____ (Constituent(s)) Date: _____

7.8 Advice surgery or interview action sheet

Date: _____ Place: _____ Time:

Name: _____ Tel:

Address _____

_____Postcode: _____

Issue to Raise: _____

Other relevant information: (addresses, phone/reference numbers): _____

_____

_____

(cont…)

(action sheet cont…)

Action required: _____

_____

To: _____ MP From: _____ Constituent(s)

Data Protection Notice

The information that you have provided on this form will only be used by (*insert MP name*) and constituency staff in relation to the issues recorded above. In order to deal with these issues it may be necessary to pass your details to third parties including, but not limited to, officials and elected representatives of local and national authorities and bodies. You should read and sign the statement below to show that you understand that your information will be used for the purpose described and that you consent to the proposed processing.

If you have any questions or concerns about how your information will be processed or about your right under the Data Protection Act 1998 please contact (*insert contact details*).

I confirm that it is my wish for you to pursue the matters I have discussed with you. In order to do so you may use all information I have provided about me, whether written or spoken, and including sensitive personal information. I understand that you will do so in accordance with the requirements of the Data Protection Act 1998.

Signed: _____ (Constituent(s)) Date: _____

7.9 Acknowledging contact from constituents

I will treat as confidential all personal information you give to me or to my staff. I may need to pass on this information to others so they can help you. I undertake to handle the information you give me in line with the requirements of the Data Protection Act 1998. If you have any queries regarding the processing of your personal data by my office, please contact (*insert contact details*).

7.10 Confirming the wishes of a constituent

You wrote to me about the case of _(*insert case details*)_. I am afraid that I am unable to take action without some evidence that this is what he/she wishes. Please send me a letter signed by this person saying that they wish me to act, or some other proof of their wishes, and I would be happy to do so.

On the other hand, if you know of a reason why this person should not be asked to give their consent, or you believe that it would be impossible to obtain it, please let me know and I will consider whether this is a special case.

7.11 Contacting others about constituency casework

I have been asked by my constituent(s) to pursue this matter and am doing so in line with the requirements of the Data Protection Act 1998. This may involve the handling of sensitive personal information, as permitted under the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002.

7.12 Response to a request to act on behalf of a non-constituent

I have noted your concerns but I am afraid that I am not able to help you directly. There is a strict parliamentary protocol that Members of Parliament do not seek to intervene in matters raised by the constituents of other Members.

If you have not already done so, I recommend that you write to your own Member of Parliament for assistance. If you are not sure who this is, ring the House of Commons Information line on **020 7219 4272** or use this website to check:
http://findyourmp.parliament.uk All you need is your postcode.

7.13 Obtaining information from other agencies

I have requested that _(*insert MP name*) _ and his/her staff to take action on my behalf with respect to _(*insert case details*)_ . I confirm that it is my wish for relevant information to be shared with my MP. This includes my personal information, *[and my sensitive personal information regarding (category of sensitive personal information)**]. I understand that any such information will be handled in accordance with the Data Protection Act 1998.

I acknowledge that it is my wish for the Member to take action on my behalf until the conclusion of this matter unless I notify the Member otherwise, and my wishes will only be reviewed if this matter is not resolved within (*insert time period*).

Name:_____ Address:_____ Signature: _____ Date:_____

**include where applicable*

7.14 Freedom of Information requests

Thank you for your letter in which you ask for access to information under the Freedom of Information Act 2000. As a Member of Parliament, I am not a public authority for the purposes of the FOIA and am not therefore obliged to respond to your request.

Optional additions

(Either) However, I am willing to disclose the requested information to you.

(Or) You may be able to access the information by contacting (insert name of public authority that may hold the requested information).

7.15 Notice to constituents from Members intending to stand down

In order to pursue the matters that you have brought to me I have retained information about your case. It is my intention to destroy all such information securely immediately after the general election when I stand down from Parliament. If you do not want this information to be destroyed, for example if you wish for this personal information to be passed on to my successor, you must write to/contact my office about this as soon as possible.

7.16 Form for constituents to indicate preference for what will happen to their case file in the event of a change in Member

I would like any records, including any sensitive information, about the issue which I have brought to _____ as my Member of Parliament to be:

(Please select one of the following options)

☐ Securely destroyed

or

☐ Transferred to the newly elected Member and their staff, regardless of who that is

or

☐ Transferred to the newly elected Member and their staff, only if it is _____ *(insert name or party)*

or

☐ Given to me, so far as this is possible*

or

☐ Other (please describe) _____

I understand that if I do not indicate a preference, my file will be securely destroyed.

** In some cases it may not be possible to pass on some records, for example if these contain confidential information supplied by another person*

A quick checklist

Do I have a policy for dealing with data protection issues?

Do I really need this information about an individual? (2.3)

Have I considered whether it is sensitive personal data and taken extra precautions if it is? (4.3)

Do I know what I'm going to use it for? (2.2)

Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for? (2.1)

Am I satisfied the information is being held securely, whether it's on paper or on computer? What about my website? Is it secure? (2.7) & (2.8)

Am I sure the personal information is accurate and up to date? (2.4)

Do I delete/destroy personal information as soon as I have no more need for it? (2.5)

Is access to personal information limited only to those with a strict need to know? (5.2)

If I want to put staff details on our website have I consulted with them about this? (2.8)

If I use CCTV, is it covered by the Act? If so, am I displaying notices telling people why I have CCTV? Are the cameras in the right place, or do they intrude on anyone's privacy? (5.5)

If I want to monitor staff, for example by checking their use of email, have I told them about this and explained why? (5.13)

Have I trained my staff in their duties and responsibilities under the Act, and are they putting them into practice? (5.1)

If I'm asked to pass on personal information, am I and my staff clear when the Act allows me to do so?

Would I know what to do if one of my employees or constituents asks for a copy of information I hold about them? (3.7)

Have I notified the Information Commissioner? Is my notification up to date, or does it need removing or amending? Section 1

Do I have satisfactory arrangements in place with 3rd party data processors? (5.2.4)