



HOUSE OF COMMONS



Data Protection

Policy and Application

July 2009

Contacts

If you have any queries or problems in interpreting or implementing the Data Protection Policy, and whenever in doubt about applying data protection in practice, please contact your Departmental Data Protection Representative (DDPR) or the Information Rights and Information Security Service (IRIS):

Department of Chamber and Committee Services

Marie Richardson x6585
Stephen O’Riordan x6391

Department of Facilities

Joanne Regan x4401
Judith Welham x4817

Department of Information Services

Paul Mann x2194

Department of Resources

Katy Gray x4296

Speaker’s Office

Peter Barratt x5300

PICT

Natalia McDonald x4174

Information Rights and Information Security (IRIS) Service

The House of Commons Data Protection Officer (DPO):

Bob Castle x2032

The House of Commons Data Protection Coordinator:

Katy Gray x4296

Contents

Foreword from the House of Commons data controller

Section I: Policy statement including roles and responsibilities

Section I of this booklet contains the Policy of the House of Commons Service for compliance with the Data Protection Act 1998. It identifies the roles and responsibilities of all managers and staff across the organisation in putting this Policy into practice.

- Policy context
- The House of Commons Service Data Protection Policy
- The Data Protection principles (listed)
- Review and audit
- Roles and responsibilities

Section II: Applying Data Protection in the House of Commons

Section II of this booklet contains guidance on day-to-day application of the Act.

- What is personal data?
- What is a data subject?
- What is processing?
- What are 'Data Protection principles'?
- The Data Protection principles (explained)
- A quick 'how to comply' checklist



Key messages for staff are highlighted in grey boxes throughout this booklet.

This booklet is supported by 'In Detail' guidance, procedures and further explanation of key terms and concepts, which is available through the parliamentary intranet at <http://intranet.parliament.uk/offices-departments/iris/>.

Foreword from the House of Commons data controller

The Data Protection Act 1998 ('the 1998 Act') has applied explicitly to the House of Commons since January 2005, although the House of Commons Service has operated as though the 1998 Act applied in full since January 2004. As Clerk of the House, I am the data controller for the House of Commons. I am therefore responsible for the application of the rights and obligations as set out in the 1998 Act to the activities of the House of Commons Service. Individual Members of Parliament are data controllers in their own right. Whilst House officials may offer guidance to Members on data protection issues, each is individually responsible for the application of the Act to their parliamentary and constituency activities.

The House of Commons Service needs to collect and use certain types of information about the people with whom it deals as part of its day-to-day business activities. These people include Members and their staff, Select Committee advisers and witnesses, current, past and prospective employees, contractors, suppliers, clients/customers and others with whom the House communicates. The House may hold this information physically (e.g. on paper records) or electronically (e.g. on computers). Such personal information must be dealt with properly, however it is collected, recorded and used. The 1998 Act establishes appropriate safeguards to ensure this is achieved.

The updated Data Protection Policy identifies the objectives of the House of Commons Service in complying with the 1998 Act. The Policy acknowledges the responsibility of all staff in implementation and outlines specific roles throughout the organisation to support the Service in adhering to the Policy. In addition to the Policy, general guidance is available for all staff on applying the Act in our daily work. This is supported by specialist guidance which explores key areas in more detail.

I have appointed a Data Protection Officer (Bob Castle) to ensure that specific responsibility for compliance with the Data Protection Act is assigned in the House of Commons Service. Additionally, each department of the House of Commons has nominated a Departmental Data Protection Representative to support the Data Protection Officer and their department. If anyone would like more information about the Act or this Policy please contact Bob Castle or any of the Departmental Data Protection Representatives.

I regard the lawful and correct treatment of personal information by the House of Commons Service as essential both to the successful management of our operations, and to maintaining the confidence in us of those with whom we deal. I will ensure that the House of Commons Service treats personal information lawfully and correctly. To this end I fully endorse and adhere to the principles of data protection, as described in the Data Protection Act 1998 and our Data Protection Policy.

A handwritten signature in blue ink that reads "Malcolm Jack". The signature is written in a cursive style with a horizontal line above the name.

Dr Malcolm Jack

Clerk of the House and House of Commons Data Controller

Section I

Policy statement, Roles and Responsibilities

This section sets out the House of Commons Service Policy ('the Policy') for compliance with the Data Protection Act 1998 ('the 1998 Act') and identifies the roles and responsibilities of all managers and staff across the organisation.

1.1 Policy context

The lawful and correct treatment of personal data by the House of Commons Service is essential both to the successful management of operations and to maintaining confidence in the Service. All House of Commons departments, offices and employees must observe and follow the provisions of this Policy to ensure that this objective is achieved. This Policy does not apply to data held by Members as they are data controllers in their own right.

The Parliamentary Information and Communications Technology Department (PICT) should comply with this policy with respect to all personal data that clearly relates to the House of Commons. PICT should comply with the House of Lords Data Protection policy with respect to all personal data that clearly relates to the House of Lords. PICT should work with reference to both policies in all other cases. In specific areas and cases, the Data Protection Officers for each House will agree which House will take the lead.

The processing of personal data is regulated by the 1998 Act. Under this Act, the Service is required to notify the Information Commissioner's Office (the Commissioner) of the purposes for which personal data is processed and to abide by eight Data Protection principles. The 1998 Act grants rights to individuals regarding the processing of their personal data and provides for exemptions to duties in certain circumstances.

There are a number of policies and programmes relating to information and data risk management, and this Policy should be read in conjunction with them. These policies include Information Security, ICT Security, Records Management, Risk Management, acceptable use policies and other guidelines, as well as guidance contained in the Staff Handbook. Information Security differs from Data Protection. The Information Security Policy focuses on technical and organisational security and it applies to any data in our possession that may cause harm or distress if it were lost or stolen, not just personal data.

1.2 The House of Commons Service Data Protection Policy

The House of Commons Service Data Protection Policy is to comply with the provisions of the 1998 Act and all relevant subordinate legislation, by:

1. Effectively and sensitively managing and processing personal data in a fair, lawful and consistent manner in accordance with the data protection principles and all other elements of the 1998 Act.
2. Establishing roles and responsibilities for compliance with the 1998 Act.
3. Developing staff understanding and awareness of their duties and obligations under the 1998 Act and the possible consequences of breaches of the 1998 Act.
4. Providing a network of key and accessible staff to assist with compliance and understanding of the 1998 Act in their local area.
5. Providing and maintaining guidance on the application and implementation of the 1998 Act to the House of Commons Service.
6. Integrating Data Protection considerations into business processes.
7. Keeping policy and practice under review.

1.3 The Data Protection principles

The Data Protection principles state that personal data shall be:

1. processed fairly and lawfully and, in particular, shall not be processed

unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is **also** met.

2. obtained only for one or more specified and lawful purposes, and shall not be further processed incompatibly with those purposes.
3. adequate, relevant and not excessive in relation to the purposes for which it is being processed.
4. accurate and, where necessary, kept up to date.
5. kept for no longer than is necessary in relation to the purposes for which it is being processed.
6. processed in accordance with the rights of data subjects.
7. protected by appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. transferred outside the European Economic Area only if there is adequate protection in the relevant country for the rights of the data subjects.

1.4 Review and audit

This Policy and supporting material will be subject to internal audit with reference to the audit materials produced by the Commissioner. They will be reviewed annually by the Data Protection Officer in consultation with the Departmental Data Protection Representatives. Consideration will be given to:

- any changes to the UK Data Protection legislation
- any new or amended guidance from the Commissioner
- any changes in current practice within the House including requirements that may involve processing of personal data on a new basis.

1.5 Roles and responsibilities

1.5.1 The Clerk of the House

The Clerk of the House is the House of Commons data controller and,

as such, is responsible for ensuring that the House of Commons Service complies with all provisions of the Act, in particular the data protection principles and notification.

1.5.2 Data Protection Officer (DPO)

The DPO (contact details on p2) is appointed by the House of Commons data controller and, assisted by the DDPR, is responsible for:

- day to day operation of the Act
- maintaining notification to the Commissioner for the House
- ensuring availability of appropriate training for staff
- provision of advice and guidance
- co-ordinating responses to requests regarding data subject rights
- monitoring complaints
- auditing the Policy and
- drafting, updating and disseminating policies and procedures with reference to developments in case law, experience and Commissioner guidance.

1.5.3 Departmental Data Protection Representatives (DDPR)

The DDPR (contact details on p2) are nominated by departments of the House to support the DPO. Within their departments, they are responsible for:

- acting as a point of contact for staff and managers
- providing advice and assistance on all aspects of the application of the 1998 Act, including handling requests regarding data subject rights
- consulting the DPO if uncertain regarding appropriate action and
- informing the DPO of all significant queries, such as those relating to new processing requirements or requests regarding data subject rights.

1.5.4 Information Security Programme

The Information Security Programme is focussed specifically on day-to-day assessment and management of information security risks, under the responsibility of the Senior Information Risk Owner. For further details, refer to the Information Security policy, which also covers the

responsibilities of the Parliamentary Information and Communications Technology Department (PICT) with respect to ICT security.

1.5.5 Managers

Managers are responsible for:

- ensuring that data protection requirements are observed
- providing clear messages to their staff regarding appropriate processing of the personal data that they handle
- identifying and addressing training needs within the team and informing their DDPG if the available training will not address their needs
- consulting their DDPG before processing personal data for a new purpose
- informing their DDPG of any data subject requests or complaints.

1.5.6 All employees

All employees are responsible for:

- complying with the data protection principles, as supported by the Policy, guidance on the application of the Policy and associated policies and guidance, such as the Parliamentary IT Security Policy and Procedures
- contacting their manager, their DDPG or the DPO for guidance if they are in any doubt about how they should deal with certain personal data
- only processing personal data in the manner that is authorised for the purpose of carrying out their job or with management authorisation.

The House takes data protection compliance very seriously; any breach of data protection legislation, local data protection procedures and/or the provisions of the Data Protection Policy may render staff liable to internal disciplinary proceedings (staff handbook <http://dfaweb.parliament.uk/hocstaff/fpandg/staffhan/shbook.pdf>). Staff should be aware that it is a criminal offence to breach certain provisions of the Act. Knowingly or recklessly obtaining or disclosing personal data without the data controller's authority may leave an individual employee liable to prosecution.

Section II

Applying the Data Protection Act 1998 in the House of Commons Service

Everyone working for the House of Commons Service is responsible for processing personal data in accordance with the 1998 Act. This section explains what this means and provides a general explanation on applying this in practice. 'In Detail' guidance, procedures and further explanation of key terms and concepts is available through the parliamentary intranet.

2.1 What is personal data?

Information will be personal data if:

1. it is personal i.e. if it is information about a living person who can be identified

This may include the individual's name, their contact details, opinions they have expressed, a record of their presence at a particular location or time or involvement in a particular activity, details of their expense claims, human resources records, development plans etc. It also includes expressions of opinions and intentions regarding the individual.

2. and it is data i.e. if it is recorded in any format.

This may be recorded in a structured format that is filed as part of the normal record of business, such as within a folder referenced by name or a database structured by individual, or any other relevant filing system. It may also be in an unstructured format, which may not be filed as a business record, such as a reference within a notebook, email or spreadsheet, photographs or CCTV footage. It includes any data held on equipment operating automatically in response to instructions (i.e. computers).

Sensitive personal data

Information will be sensitive personal data if it is personal data about a data subject's racial or ethnic origin; political opinions; religious beliefs

or beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; commission or alleged commission of any offence and information about any associated proceedings.



If staff are not sure whether information they are handling is personal data or whether it is being processed, their Departmental Data Protection Representative or the Data Protection Officer can give advice.

2.2 What is a data subject?

A data subject is any individual who is the subject of personal data. For example a specific Member or their staff, a Select Committee adviser or witness, a current, past or prospective employee, a contractor, supplier, client/customer or any other person with whom the House communicates.

2.3 What is processing?

Processing covers any action that can be done with data. This includes obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, using, transferring, disclosing, aligning, combining, transcribing, printing, filing, sorting, blocking, erasing or destroying data.

2.4 What are 'Data Protection principles'?

The eight data protection principles are the most substantive part of the Act and represent the core duties imposed on the House of Commons. They apply to all personal data held by the House of Commons, regardless of the format in which it is held or whether it is held centrally, within different departments or by individual employees.



Everyone in the House must apply the eight data protection principles to any personal data they process in their daily work. The following pages of this booklet identify what the Act says for each principle, explains what this means for staff operating in the House of Commons Service and, where possible, gives relevant examples.

In very exceptional circumstances, one or a number of the principles may not apply as a result of specific exemptions identified in the 1998 Act. An example would be if personal data must be processed to prevent or detect crime and complying with the principles would prejudice that purpose.

If there is any reason why staff believe it to be inappropriate or impossible to comply with any of the data protection principles, they must inform their DDPR **before** processing the personal data. The DDPR will consult with the DPO and Legal Services Office to ascertain on a case-by-case basis whether an exemption applies and will advise the staff regarding the appropriate action to take.

2.5 The Data Protection principles

The first Data Protection principle states that personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The first principle is also the most complex, as it contains a number of different requirements.

Fair processing

Firstly, personal data must be processed fairly. This means that:

- The data subject must be informed of who is processing their personal data and why (this should include the identity of the data controller and is referred to as a ‘data protection notice’ or a ‘fair processing notice’)
- The data subject must not be misled as to what their data will be used for, including who will have access to it and that they may contact the DPO with queries or complaints regarding the processing of their data.
- The data subject must be able to judge how much personal data they wish to provide according to the use that the data will be put to and be able to exercise their rights under the 1998 Act.

A data subject must be given a ‘data protection notice’, usually before or at the time that the House begins to collect their personal data. Detailed guidance is available on the parliamentary intranet on how to use ‘data protection notices’.

Legal processing

Secondly, personal data must be processed lawfully. Generally, this means that it must not be processed if doing so would be in breach of any law or legal obligation, such as the common law duty to protect confidential information.

Satisfying certain conditions

Thirdly, personal data may only be processed if certain conditions are met. In the case of personal data, one condition from a specific list contained in Schedule 2 of the 1998 Act must be met before the personal data can be processed. These conditions include:

- consent from the data subject
- processing that is required by a legal obligation
- processing which is in the legitimate interests of the data controller where the data subject’s rights and legitimate interests will not be prejudiced by the processing.

In the case of sensitive personal data, a further condition from Schedule 3 of the 1998 Act must also be met in addition to meeting a condition from Schedule 2. A full list of the Schedule 2 and Schedule 3 conditions is available in guidance on the parliamentary intranet on satisfying relevant conditions.

It is not always necessary to obtain consent from data subjects to be able to process their personal data. There may be other conditions that can be satisfied to permit processing. Guidance is available through the parliamentary intranet which goes into more detail about seeking consent.



Guidance should be sought from your Departmental Data Protection Representative if there are any queries regarding whether processing of personal data is in accordance with the first data protection principle.

Examples:

- Individuals whose personal data will be processed in the context of the activities of a particular Select Committee should be informed what will be done with their personal data. This should include whether it will be included in minutes or other documentation, whether it will be published and whether it will be passed on to other Select Committees, departments of the House or external bodies including the House of Lords.
- Employees should be informed what will happen with their personal data that is held by the House. This should include regular and irregular processing, such as whether it may be passed to tax authorities, police or lawyers outside the House if there is a duty on the House to do so, for example to support criminal investigations. The Staff Handbook contains much of this information.
- Managers providing references or reports about their employees should be informed whether their opinions and intentions as contained in these reports may be shared with others including their employees.

The second Data Protection principle states that personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed incompatibly with those purposes.

This means that the House of Commons must identify the reason why it obtains and processes personal data. This must be done in two ways:

1. Through 'data protection notices' to data subjects

'Data protection notices' are explained under the fair processing section of the first data protection principle. Personal data should not be processed for purposes outside those identified to the data subject through a 'data protection notice'. Detailed guidance is available through the parliamentary intranet on using 'data protection notices'.

2. And through notification to the Commissioner.

The House of Commons Service is required to provide the Commissioner with certain details about its processing of personal data and the name and address of the data controller. The House of Commons Service's notification must reflect, at any given time, its operations involving processing of personal data.

The purpose of notification is to assist the public in understanding what information the House of Commons Service processes and for what reasons. The House of Commons notification reference is Z8887540 and can be viewed at <http://www.ico.gov.uk/ESDWebPages/DoSearch.asp>.

The DPO is responsible for maintaining the House of Commons' notification. Notification must be reviewed annually and updated within 28 days of any changes. Failure to have a notification entry and failure to keep it up-to-date are criminal offences.



Managers must contact their Departmental Data Protection Representative if they have a business need to process personal data for a new or different purpose.

All processing of personal data within the House of Commons Service must be in accordance with the purposes identified in its notification and data protection notices.



Staff must only use, disclose and otherwise process personal data for the particular purpose for which that data was originally obtained. Particular care should be taken when passing personal data to other departments, Select Committees, offices or sections.

Using personal data for new purposes

There may be circumstances when the House of Commons Service, in accordance with its legitimate needs, wishes to use or process personal data for purposes that were not envisaged at the time when the personal data was originally obtained and processed. This may be within the department that originally processed the data, or a different department.



Managers must consult their Departmental Data Protection Representative before processing personal data for a new purpose. Consideration will need to be given to:

- Satisfying appropriate conditions for fair and lawful processing;
- Informing the data subjects what the planned new uses of their personal data are and seeking consent / offering them an opportunity to object where relevant; and
- Complying with all the other principles.

Detailed guidance is available for managers through the parliamentary intranet.

For example:

- Personal data obtained in the process of recruitment and employment with the House should only be used in a way which is compatible with recruitment and employment purposes. This personal data should not be used for other purposes, such as identifying someone's birthday and home address in order to send them a birthday card.
- Personal data which the House of Commons Service obtains from advisers for the purpose of assisting in an inquiry or review should only be used for that sole purpose. It should not be further held and processed for some other reason, such as producing a Library Research Paper or any other briefing.

The third Data Protection principle states that personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed.

This means that all personal data held by the House must be sufficient for and closely related to the purposes for which they are processed.



- Only use the minimum necessary information in any processing of personal data
- Anonymise or abbreviate personal data if it is possible to do so in relation to the purpose for which it is held, for example when analysing responses to a questionnaire
- Do not collect or retain personal data on the basis that it may prove useful for an undefined purpose in the future
- Any irrelevant or out of date material should be deleted from files if there is no justifiable reason to retain it (see principle 5)
- Staff developing application forms, questionnaires and any other forms for collecting personal data must ensure that no more information is sought than is necessary. Essential and optional fields must be clearly marked. Before being used in practice, these forms should be submitted for assessment and evaluation to a relevant Departmental Data Protection Representative.

For example:

- Personal data obtained in the course of recruitment must be limited to what is necessary to evaluate the suitability of prospective candidates and their career potential. Collecting personal data on the employees' family members (except for security clearance) or their health is likely to be excessive and not relevant to recruitment purposes.
- Managers and Human Resources must limit the amount of personal data held on employees to that which there is a justifiable need for them to hold to maintain appropriate employee records. This may include data on absence, performance or relevant experience.

The fourth Data Protection principle states that personal data shall be accurate and, where necessary, kept up-to-date.

This means that reasonable steps should be taken to ensure the accuracy of personal data when it is received or used. Where appropriate, it also requires the accuracy of personal data to be maintained. This will be more important with live records and is less likely to be appropriate with closed or historic records.

Inaccurate data may disadvantage an individual in some cases. A data subject has the right to request that their personal data be rectified, blocked, erased or destroyed. This applies whether or not the data accurately record information received or obtained by the data controller from the data subject or third party.



Staff responsible for processing personal data must:

- Make sufficient enquiries when personal data are not obtained directly from the data subject to ensure that the House can be reasonably sure of the accuracy of the information. Where possible, accuracy should be confirmed with the data subject.
- Regularly update and review the accuracy of that personal data.
- Promptly correct inaccurate data as soon as it is identified, both where it has been identified by someone within the House and on request from the data subject concerned.
- Contact their Departmental Data Protection Representative if there are any reasons why it would be inappropriate or impossible to amend data that is known to be inaccurate.
- Where suitable, make appropriate efforts to inform other departments or external third parties to whom the data has been disclosed of any inaccuracies.
- Take appropriate steps to ensure personal data is up to date whenever any decision is to be made based on the personal data that is held.

Where personal data are held and shared between different departments, as may be the case with Human Resources records, the sharing departments should adopt a uniform and consistent policy on up-dating and maintaining such parallel records.

The fifth Data Protection principle states that personal data shall not be kept for any longer than is necessary.

This means that personal data should only be kept for as long as is necessary for the purpose for which it was obtained. If the personal data has been further processed for a subsequent purpose (see principle two), it should only be kept for as long as is required for both purposes.

In certain circumstances, there may be a good reason to retain personal data even after the original purpose for holding the data has concluded. For example, when the employment of an employee is terminated the House may still need to retain the personal data of a former employee for pension purposes or to defend any legal action brought by that individual. Before destroying personal data it is necessary to consider whether it must be retained for a legitimate future purpose.



Staff responsible for processing personal data must:

- Manage it in accordance with the Parliamentary Records Management Policy
- Dispose (i.e. destroy or transfer to the Parliamentary Archives for permanent preservation) in line with the Authorised Records Disposal Practice.
- Ensure that all surplus copies of personal data are erased in accordance with the Authorised Records Disposal Practice at the same time as master copies.
- Contact their departmental Record Officer or the Records Management Team if they hold records that do not have a retention period identified in the Authorised Records Disposal Practice to ascertain how long they should be retained.

If there is a business purpose for doing so, departments may be able to keep statistical and otherwise anonymous data for longer than the personal data that information is based on, providing there is no link between such data and an identifiable individual.

Personal data that has been identified by the Parliamentary Archives as being of historical importance may be retained indefinitely if it is held only for historical purposes (section 33) even if the business purpose for keeping the records has expired.

The sixth Data Protection principle states that personal data shall be processed in accordance with the rights of data subjects.

Data subjects have a number of rights under the 1998 Act regarding their personal data. These rights are detailed below. The House must ensure that:

- data subjects can exercise their rights
- requests from individuals are dealt with swiftly and without undue delay
- exemptions to data subject rights are applied correctly and
- appropriate records are made of our response to requests from data subjects.



Any member of staff who receives a request or a complaint from a data subject regarding any of these rights should immediately inform their Departmental Data Protection Representative of the request. The request can then be handled according to the procedure for processing data subject requests, which can be found on the intranet.

The right of access to personal data (a Subject Access Request) is contained in section 7 of the Act

Every data subject may request access to their personal data to enable them:

- to check the accuracy of this data and
- to ensure that it has been collected, held and otherwise processed in accordance with the law.

A data subject may request in writing:

- to be informed whether their personal data is being processed by the House;
- to be given a description of their personal data, the purpose(s) for which it is being processed and the recipient(s) to whom they may be disclosed;

- to have communicated to them in an intelligible form the personal data of which they are the subject and any information the House has as to the source of the data;
- to be informed of the logic behind any automated decision taking (see below for an explanation of automated decision taking).

It is not currently our policy to charge a fee for Subject Access Requests.

The right to prevent processing likely to cause damage or distress is contained in section 10 of the Act

Every data subject has the right to object at any time to processing of his/her personal data, where such processing may cause substantial and unwarranted damage or distress.

The right to prevent processing for the purposes of direct marketing is contained in section 11 of the Act

Any data subject has the right to object to direct marketing and the House must comply with such requests as quickly as possible. Direct marketing covers communication by any means of advertising or marketing material to particular individuals, including offers of goods or services and promotion of aims or ideals. This right is further supported by the Privacy and Electronic Communications Regulations (EC Directive) 2003.

Rights in relation to automated decision taking is contained in section 12 of the Act

Sometimes organisations will use a computer to process personal information about an individual, in order to take a decision that will affect them. For example, an employer who uses computer scoring of job applications to decide who to interview, or a bank who uses a computer to assess an individual's eligibility for a mortgage or loan application. In some circumstances, an individual may have the right to prevent decisions being taken about them which are based solely on automatic processing. It is likely to be uncommon that decisions will be made solely by automated means within the House.

The right to compensation for failure to comply with certain requirements is contained in section 13 of the Act

Any data subject may claim compensation through courts for any damage suffered as a result of a breach of any of the requirements of the Act. Data controllers can avoid liability by proving that they have taken reasonable steps to comply with these requirements.

The right for inaccurate or misleading data to be rectified, blocked, erased to be destroyed is contained in section 14 of the Act

Any data subject may apply to court to request that the House, or any of its departments, rectify, block, erase or destroy any personal data which are inaccurate, i.e. incorrect or misleading or contain information and/or opinions which are based on inaccurate data. The court may also order the data controller to notify any third parties to whom the data in question may have been disclosed of the rectification, blocking, erasure or destruction.

Additionally, any person directly affected by any processing of personal data may apply to the Commissioner in accordance with section 42 of the Act for an assessment as to whether this processing has been carried out in compliance with the Act.



Members of staff

Members of staff have the right to exercise any of the above rights. If they wish to do so, they should contact their manager, their Departmental Data Protection Representative or the Data Protection Officer and explain which right they wish to exercise. It may be necessary for the request to be made in writing.

Exemptions to data subject rights

The policy of the House is to promote transparency and openness in personal data processing operations. Allowing data subjects to exercise

their rights is an important part of that policy. We should make our best efforts to supply the data subject with requested information in response to access requests and should give effect to requests for us to amend our processing of their information in appropriate cases.

Exemptions to these rights should be relied upon only in exceptional circumstances. In general, exemptions should be claimed where giving effect to the request would prejudice the interests and operations of the House. Further detail on the application of exemptions can be found in detailed specialist guidance through the parliamentary intranet.



In all cases, advice should be sought before seeking to apply any exemptions to requests to exercise data subject rights.

The seventh Data Protection principle states that personal data shall be protected by appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

This means that personal data must be stored and handled confidentially and securely. Care must be taken at all times, from when the data is originally obtained right through to when it is ultimately destroyed. Possible protective measures include using logins, password protection, encryption, locking papers away and locking workstations when unattended and not taking papers or portable data devices away from the office without adequate protection. Particular care must be taken with electronic information, such as emails.



The security framework

- All staff have a duty of confidence to protect sensitive information.
- If staff are unclear as to what action is necessary to keep data secure, they must discuss with a manager and, if necessary, their Departmental Data Protection Representative.
- Managers must ensure that staff are aware of and comply with security procedures. This includes non-permanent staff permitted access to personal data.
- Managers must adopt measures to ensure the integrity of staff through selection, training, supervision and motivation. This includes non-permanent staff permitted access to personal data.
- Access controls, both physical and logical, must be implemented and appropriate audit trails put in place in all areas where personal data are processed.
- PICT Security Policies and Procedures and other information security policies and procedures must be followed at all times.

Appropriate security measures may differ according to the nature of the data concerned. For example, health or disciplinary records will generally require a greater degree of protection than a list of internal contact details. In assessing the appropriate level of security, consideration should be given to:

- the risks involved in various processing operations
- the nature of personal data
- options for technical protection
- the harm that might result from a breach of security
- ensuring the reliability of the staff having access to personal data

Data processors

If personal data is to be processed on behalf of the House by an outside organisation (a data processor), the House must:

- choose a data processor that provides adequate guarantees regarding the technical and organisational security measures for the personal data they will be processing;
- take reasonable steps to ensure the data processor is complying with those measures;
- establish the above in contract where appropriate.



Staff must notify their Departmental Data Protection Representative (DDPR) if they intend to use a data processor. Advice may be required from the DPO, Legal Services Office and Procurement on establishing contractual relations with the processor.

The eighth Data Protection principle states that personal data shall not be transferred outside of the European Economic Area (EEA) without adequate protection

This means that personal data must not be sent outside of the European Economic Area (the European Union plus Iceland, Lichtenstein and Norway) unless certain measures are put in place.



Any member of staff must notify and consult with their DDPR if they are considering transferring personal data to a country or territory based outside of the EEA.

Personal data placed on websites, including text and photographs, are effectively transferred outside of the EEA as the information may be accessed and used anywhere in the world. It may be necessary to seek consent from the data subject specifically for this transfer before their data are to be uploaded to an external facing website.

A quick 'how to comply' checklist

This checklist should help you with the Data Protection compliance when handling information about people. Being able to answer 'yes' to every question will not guarantee compliance, but it should mean that you are heading in the right direction.

For all staff:

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- 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?
- Am I satisfied the information is being held securely, whether it's on paper or on computer?
- Am I sure the personal information is accurate and up to date?
- Do I delete/destroy personal information as soon as I have no more need for it, in line with the Authorised Records Disposal Practice?
- Is access to personal information limited only to those with a strict need to know?

For managers:

- Have I made sure my staff are trained in their duties and responsibilities under the Act, and are they putting them into practice?
- If I want to put staff details on our website have I consulted with them about this?
- If I want to monitor staff, for example by checking their use of email, have I told them about this and explained why?
- 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 individual customers asks for a copy of information I hold about them?