Chapter 23: Handling Information

1. About this Chapter

1.1. This chapter covers handling information in accordance with our legal obligations and how to meet the House of Commons’ responsibilities to keep information secure. This includes:

- Managing information - Information Rights
  - Freedom of Information (FOI) / Environmental Information Regulations (EIRs)
  - Data Protection
  - Information about you
  - Legal obligations regarding personal data

- Protecting information - Information Security
  - Your responsibilities
  - Parliamentary Protective Marking Scheme
  - What to do when information is compromised
  - Where to go for help or further advice

2. Managing information- Information Rights

FOI and EIR

2.1 FOI & EIR covers all recorded information held by a public authority. This includes business materials held in personal areas such as your inbox, personal drives and memory sticks and any other solutions or applications you use on your own devices for business purposes, such as WhatsApp or Gmail.

2.2 Anyone, anywhere in the world can request information held by the House of Commons and there are limited exemptions to disclosure of the information. It is important we know where information is so we can access it quickly and that our records are complete and up to date. Please ensure you follow good records management practices and policies such as the Authorised Records Disposal Practice (ARDP). FOI and EIR requests received by the House are managed by the Information Rights and Information Security (IRIS) Service.

2.3 If you receive a request for information under FOI or EIR, you should notify IRIS by email: FOICommons@parliament.uk. To comply with legislation, a response must be provided within 20 working days. More information about FOI/EIR processes and your responsibilities are available on the FOI pages on the Intranet.

2.4 The House also releases information proactively as part of its publication scheme. You should bear in mind that a wide range of information about the business and employees of the House may be released, including items which the House of Commons requires to be registered centrally.
Data Protection

2.5 The House of Commons is obliged to handle information in accordance with Data Protection Legislation; the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA). These laws set out the principles and lawful bases that personal data must be managed in line with and provide a flexible, risk-based approach which puts the onus on each of us to think about and justify how and why we collect and use personal data.

2.6 These laws also provide certain rights to individuals. These include the right to be informed about how personal data is used and who it is shared with (privacy notices), the right to access personal data and the right to object or restrict processing.

2.7 Anyone can request access to their own personal data which is held by the House. This is called a Subject Access Request (SAR) and must be answered within one month of receipt. If you require access to information about yourself, you should make a request to the person or team who holds the information, such as the HR team. If you have a larger or more complex request (for example, if you think several teams hold your personal data) please make your request to IRIS.

2.8 Further information about data protection is on the Intranet at: Data protection and security. You can also find out more about your rights from the Information Commissioners Office, who are the supervisory authority for the UK.

3. Information about you

3.1 There may be occasions where we may share or disclose personal data about you as an employee of the House, some examples are included below, though this list is not exhaustive:

- Your name, job title and business contact details may be published on the Parliament website if you are a senior manager or work in a customer facing team. Please note: if you post details about your role in the public domain, on sites such as LinkedIn or Twitter, it makes it harder for the House to refuse to disclose this information if asked (for example as part of a FOI request).

- We may be asked to provide staff details as part of a request. In general, the more senior you are, the more information we may disclose. Please note: personal details that are already publicly available, such as names and contact details of Committee staff on a Committee web page, will be routinely disclosed upon request.

- We require some personal data for business continuity purposes. It may be used for the purpose of contacting you in the event of an emergency. In addition, if you have
an extended period of absence, especially at short notice as a result of an accident, your line manager may be given access to your business work areas (such as your email account) to ensure the continuity of any work you were involved with.

- For the purpose of investigating grievance or disciplinary matters, we may share some of your personal data such as pass access records, email or internet use records, electronic key data, etc. with your line manager or another investigating manager. Some personal information may also be shared with the Police if it is required for the purpose of investigating whether a crime has been committed.

3.2 Your personal data will only be used, shared or published where it is lawful to do so in line with data protection legislation. More information about the use of staff information can be found in the staff privacy notice on the intranet. If you have any queries or concerns, please contact your line manager or IRIS.

National Fraud Initiative and Data Analytics

3.3 The House of Commons participates in the National Fraud Initiative (NFI) and undertakes internal data analytics for assurance and counter fraud purposes. The National Fraud Initiative is a data matching exercise that compares information held by, and between, around 1,300 public sector organisations. The aim of the initiative is to help identify potentially fraudulent claims, errors and overpayments.

Data matching involves comparing sets of data held by one organisation with records held by the same or another organisation to see how far they match. This will include personal information of staff and suppliers. Inconsistencies or anomalies identified through this exercise do not necessarily indicate fraud, but they may require further investigation. Further information on the National Fraud Initiative is available on the Cabinet Office website and in the staff notice available on the intranet.

Honours

3.4 We are proud that a number of our staff, past and present, have received honours from the Crown. If you are nominated for an honour, then we may be required to provide your personal data to the Cabinet Office for that purpose. This may include some sensitive data such as your gender and nationality. The Cabinet Office strictly stipulate that nominees may not be informed that they are being considered, so we would not be able to notify you that this information was being shared at the time.

If you would not want us to share your data for this purpose (and this means that you would never be nominated for an honour), please:

I. Inform Payroll Services who will make a note on your file.
II. Inform your line manager - they would be asked to provide information as part of any nomination process so will need to know that you would not want this to
happen. If your line manager changes, it is your responsibility to inform your new manager of your decision.

4. Legal obligations regarding personal data

4.1 As well as providing individuals with certain rights, data protection legislation also includes responsibilities for the protection and lawful use of personal data (data that identifies living individuals). These laws govern how we ‘process’ personal data, for example, holding, obtaining, recording, using and sharing. If you knowingly contravene the DPA, disciplinary action may be taken against you.

4.2 The Clerk of the House is the data controller of personal data held by the House of Commons and the Data Protection Officer is the Head of IRIS. The Senior Information Risk Officer (SIRO) is the senior person responsible for overall information assurance for the House of Commons at Board level. The Managing Director of Research and Information is the SIRO.

4.3 All staff are required to handle individuals’ personal data appropriately, with respect for those individuals’ privacy and their rights. You must not:

- Collect, process or store personal data without the proper authority or consent to do so
- Share personal information without the correct authority or consent to do so
- Keep personal data for longer than is required.

4.4 The IRIS team provide data protection training and advice for staff. An e-learning training module ‘Data Protection for staff’ is available on ACT. Further information is also available on the Intranet.

5. Protecting information - Information Security

What is information security?

5.1 Information security is about treating information appropriately and keeping it safe. This is crucial when handling sensitive information.

What is sensitive information?

5.2 Sensitive information is information in any format (hard copy or electronic) where in the event of a loss or compromise it would:

- Disrupt operations and services
- Damage the reputation of either House
- Place individuals at risk for example, from identity theft, fraud or acts of terrorism
- Breach confidentiality
- Affect personal security or privacy
5.3 Sensitive information must be protected. This includes:

- Keeping hard-copies or devices containing sensitive information (USBs, etc.) locked away
- Controlling access to electronic copies with secure access groups/permissions and/or password-protection
- Not taking it off the parliamentary estate without appropriate permission and working securely when working away from the Parliamentary Estate.
- Never sending it to personal email accounts or social media tools
- Applying the Parliamentary Protective Marking Scheme
- Thinking before you share sensitive information and sharing it securely.
- Where possible, share links rather than send attachments

What is the Parliamentary Protective Marking Scheme?

5.4 The Parliamentary Protective Marking Scheme is a mandatory policy you must use to let people know that the information they are handling is sensitive in nature. The information should be clearly labelled “RESTRICTED ACCESS” or “RA” along with a descriptor. For further information please ask your line manager, Departmental Information Risk Owner (DIRO), or read the details available on the intranet.

Register of Sensitive Information Assets (RSIA)

5.5 The Register of Sensitive Information Assets (RSIA) provides an overview of the more sensitive types of information handled within the organisation and details the arrangements in place to keep it secure. This document is managed by your Departmental Information Risk Owner (DIRO).

Data Maps

5.6 Similar to RSIA, each Team maintains a Data Map of the personal data assets which is a requirement of the General Data Protection Regulation (GDPR). The data map is managed by your DIRO.

Using approved ICT solutions

5.7 Parliament has an accreditation process in place to provide assurance that technical solutions, storing or processing parliamentary data, are meeting appropriate security standards. You must only use tools that have been formally approved for use. For further details please see Information Security Accreditation.

5.8 You should familiarise yourself with the Acceptable Use of Parliamentary Digital Services – User Responsibilities. This document sets out your responsibilities when using parliamentary digital services. It covers both devices you own and those provided by Parliament.
What to do when information is compromised

5.9 If information is destroyed, lost, altered without authorisation or accidentally disclosed to another party this is classed as an information breach. If personal data is involved, the House Service has 72 hours to report this to the supervisory authority, Information Commissioners Office (ICO), who oversee data protection laws.

5.10 If you think you are responsible for a breach or have identified a breach, ACT QUICKLY:
- Report to IRIS (House of Commons) immediately. This can be done via email or through the equipment/information loss form on Digital Support Online.
- You should inform your line manager and/or Departmental Information Risk Owner (DIRO) who will be able to offer advice and help mitigate any harm.
- Further details can be found on the Information Breach intranet page.

6. Where to go for help and further advice

You can get help and support from:

Information Rights and Information Security (IRIS)

6.1 IRIS can help you make the right decisions about processing, protecting and disclosing information and data you are required to work on. They can be contacted via email: iris@parliament.uk or ext. 2559/8805. You can also visit the IRIS intranet pages for guidance.

Departmental Information Risk Officer (DIRO)

6.2 Each Team has a designated DIRO. The DIRO has overall responsibility for information risk assessment, handling and investigating information breaches, monitoring and mitigation and provides assurance that business practices accord with policies and guidance.

7. Data Protection Officer (DPO)

6.3 The GDPR requires a public authority to appoint a data protection officer. The DPO assists in monitoring internal compliance, provides advice and assistance on data protection laws and the House’s obligations and acts as a contact point for data subjects and the supervisory authority, the Information Commissioner’s Office (ICO). If you have any queries or concerns about data protection, the Data Protection Officer for the House of Commons is the Head of IRIS.

Return to the Staff Handbook.