Chapter 23: Information Security Responsibilities

1. About this Chapter

1.1. This chapter provides information about handling information and how to meet the House of Commons obligations in keeping information secure. This chapter will cover:

- what is information security
- legal obligations relating to information
- what is sensitive Parliamentary information
- handling and protecting sensitive information
- what to do when information is compromised
- where to go for help or further advice.

2. What is Information Security?

2.1 Information security refers to the security of all of the information held by an organisation. The terms 'data protection' and 'data security' are also frequently used, often interchangeably. However, it is important to know the difference between them.

2.2 Data or information security tends to be used to describe the wider technical and organisational measures that the House needs to take to look after the information in its possession, no matter how it is held. This is particularly important for any sensitive information which may cause harm or distress to an individual, or compromise the House if it was lost, stolen, tampered with, or accessed without authorisation.

2.3 Information and data are key business assets. The House of Commons Service needs to collect, use and manage information as part of its day-to-day business activities.

2.4 Further details are on the Intranet at: Information security

3. Legal Obligations Relating to Information

Data protection

3.1 Data protection is concerned with the protection and lawful use of personal data (data about living individuals) under the Data Protection Act 1998.

3.2 The House is obliged to comply with the principles set out in this Act, which sets conditions for processing personal data, for example, holding, obtaining, recording, using and sharing. The Act protects individuals if they can be identified from that data or from that data along with other information.

3.3 The Act applies to all personal information regardless of its format or organisation, including paper and electronic, structured and unstructured records. It therefore covers HR records and

records held on employees. It also covers some information held on other individuals such as Members and constituents.

3.4 The Clerk of the House is the data controller of the personal data held by the House. All staff are required to handle individuals' personal data appropriately, with respect for those individuals' privacy and their rights regarding information about themselves.

3.5 You MUST NOT:

- gain access to personal data whether on paper or on a computer or use the data unless you have proper authority
- allow another person to access personal data or pass it to them unless you have proper authority
- destroy personal data unless you have proper authority.

3.6 If you knowingly contravene the Data Protection Act 1998 disciplinary action may be taken against you.

3.7 You are entitled to ask to see any personal data that the House holds about you. The House will allow you to see this information unless there is a legal reason why you should not see it, such as if it includes legal advice and references of a confidential nature. If you wish to see any information you should send a written request to the person who holds the information, usually the Information Rights and Information Security team (IRIS).

3.8 If providing you with a copy of the information would involve disproportionate effort you may be allowed to see any file or information held about you, rather than receiving copies of specific documents.

3.9 A copy of the House of Commons Data Protection Policy is on the Intranet at: Data Protection

Freedom of Information (FOI) and Environmental Information Regulations (EIR)

3.10 Under the Freedom of Information Act 2000 (FOI) people have the right to request information from public authorities, which includes the House.

3.11 You may, in your role, have to respond to requests in accordance with the Act. Under the Act people have the right to request information from public authorities. The information must be provided within 20 working days unless the information sought is in an exempted category. All requests for information are covered by the Act if they are in writing, including emails and faxes.

3.12 Enquiries, including those received by phone, on topics such as energy consumption and waste disposal will need to be considered separately under the Environmental Information Regulations (EIR). Those regulations are more fully explained in our FOI guidance which is on the Intranet at:

FOI guidance

3.13 FOI or EIR requests received by the House are managed by IRIS under the guidance of the Managing Director of Information and Research. If you receive a request for information under FOI or EIR, you should notify the IRIS team on ext. 8805 or email FOICommons@parliament.uk.

3.14 Detailed guidance about handling a request is on the Intranet at: FOI guidance

3.15 When information could be and is routinely requested, for example, by journalists, the House may release such information proactively as part of its publication scheme. You should bear in mind that a wide range of information about work or employees may be released, including items which the House of Commons requires to be registered centrally.

Information about you

3.16 Under the FOI Act the House may be required to release information about you. For example, if the House is asked for the names of senior staff, their pay band, job functions, interests or decisions they have made in their official capacity, then this would normally be released.

3.17 On the other hand, information such as home addresses or internal disciplinary matters would not be volunteered and would be disclosed only in exceptional circumstances and after consultation with the member of staff concerned, if such disclosure was required by the Act.

3.18 If you have any concerns about your name or any other information about you in your official capacity being made public, you should talk to your Line Manager.

3.19 Further information about data protection is on the Intranet at: Data protection and security

4. Handling and Protecting Sensitive Information

What is sensitive Parliamentary information?

4.1 Any information that you access for work purposes may potentially be sensitive Parliamentary information. The scope should be interpreted broadly. The test of sensitivity relates to information in any format, hard copy or electronic, where the loss of it may:

- adversely risk the smooth running of operations and services
- damage the reputation of either House
- place individuals at risk for example, from identity theft, fraud or acts of terrorism
- potentially breach confidentiality
- affect anyone's personal security or privacy

4.2 Some examples are:

- personal information about living individuals including names, payroll details, staff performance and appraisals, disciplinary and other personnel matters
- sensitive personal information about individuals, for example, health information such as sickness records or union membership
- business continuity information, for example, detailed business recovery plans or contact cascades

- procurement bids and contractual details, internal business cases and project board discussions
- financial or business data
- statistical profiles and responses
- draft select committee reports and evidence
- administration working papers, including minutes and agendas
- risk assessments and consultancy reports
- detailed Estate layouts and security plans.

4.3 You should bear in mind that information may become more or less sensitive throughout the stages of the work in progress. You should consider its relative sensitivity and security at all stages, and whether two pieces of information may be more sensitive when combined.

Your responsibilities

4.4 In handling and protecting sensitive information you are expected to act with caution at all times and follow the advice and guidance below.

4.5 All Parliamentary staff are responsible for protecting information, both paper and electronic, and keeping the Parliamentary network safe. Staff must familiarise themselves with and follow the relevant policy and procedures on information security.

4.6 Taking unnecessary risks with sensitive Parliamentary information may harm the reputation of Parliament and/or the safety and privacy of individuals.

4.7 Any non-compliance with the policy and guidance in this chapter may lead to disciplinary action being taken against you.

4.8 More information on handling and protecting information is on the Intranet at:

Information security

Protective Marking Scheme

4.9 The bicameral Parliamentary Protective Marking Scheme is an important element of the information security responsibilities shared by all staff and its application is mandatory across the administrations of both Houses.

4.10 The scheme consists of only one level of marking for documents that need protection. This level is **RESTRICTED ACCESS.** It is used along with a descriptor, for example, **MANAGEMENT** or **PERSONAL DATA**, to describe the nature of the information. The use of the marking will set minimum standards of care in terms of storage, handling and transfer of both paper and electronic information. It will alert recipients that it is sensitive and must be handled appropriately.

4.11 It is your responsibility to:

- be familiar with the scheme
- correctly mark information requiring protection under the rules of the scheme

- apply the appropriate handling requirements to restricted access information that you create or receive
- notify your Line Manager of any issues that may be obstructing you from applying the scheme effectively
- Notify your Line Manager immediately if any protected information may have been compromised.

4.12 Any non-compliance with the policy and guidance in this chapter may lead to disciplinary procedures being taken against you.

4.13 More information about the scheme is on the Intranet at:

Parliamentary Protective Marking Scheme

Register of Sensitive Information Assets (RSIA)

4.14 The Register of Sensitive Information Assets (RSIA) will provide an overview of the more sensitive types of information handled within the organisation, state who has access, including third parties, and the arrangements in place to keep it secure.

Protection of sensitive information beyond the Parliamentary Estate

4.15 Loss or inappropriate disclosure of sensitive Parliamentary information can occur through theft, negligence or malicious misuse, when commuting to and from the estate, working in a public place or even in your own home.

4.16 The Board has agreed that sensitive parliamentary information being removed or transferred for processing away from the Parliamentary Estate in hard copy or on electronic storage devices poses the greatest risk to information security.

4.17 You must seek authority from your Line Manager before taking any sensitive information away from the Parliamentary Estate.

4.18 Managers must take all reasonable steps to ensure that staff are not required to remove sensitive Parliamentary information from the Estate unless it is absolutely necessary. You are expected to consider the scope to rearrange existing duties to allow staff to work on sensitive information within the secure environment of the Estate in the first instance.

4.19 Authority should be given only where there is a clear business need to do so and steps have been taken to minimise the risks and mitigate the impact of loss.

4.20 You must ensure that sensitive Parliamentary information is protected by appropriate security to guard against its loss or inappropriate disclosure. As a rule:

- only the minimum amount of information required for the business need should be taken off the estate
- remove as much sensitive information, from documents, as is practicable, for example, by removing individuals' names

- transport paper documents in sealed envelopes marked with a return address, preferably within locked briefcases or bags, and not within clear plastic document wallets where the contents may be seen
- lock away documents at your home or final destination when they are not being worked on
- take great care when commuting or travelling on public transport that documents and electronic devices are not overlooked, mislaid or left unattended for any part of the journey
- follow Parliamentary ICT Security Policies and Procedures on protecting electronic information, for example, remote access and use of encrypted memory sticks (see chapter 22).

4.21 Further tips and best practice on the handling of sensitive Parliamentary information are on the Intranet at: Information security

4.22 Further tips and best practice on safer remote working are on the Intranet at:

Tips for safer remote working

4.23 Authorisation is required before forwarding official documentation to private email accounts or using externally-provided services for the production and/or storage of official data or documentation. You should never set-up automatic arrangements for forwarding work-related emails to a private or external email address.

4.24 The policy on the use of mobile devices (via Active Sync) can be found on the Intranet at:

Use of mobile devices (via Active Sync)

4.25 The purpose of the policy is to set out your responsibilities when using mobile devices to access Parliamentary information. It covers both devices you own and those provided by Parliament.

5. What to Do When Information is Compromised

5.1 Any loss or compromise of sensitive Parliamentary information is a serious matter and it is essential that the following guidance is followed.

5.2 This procedure applies to the loss or theft of any Parliamentary information in electronic or paper format and/or loss or theft of equipment. It may also be applicable to a temporary loss if the information is considered sensitive.

5.3 The following actions must be taken promptly. Do not delay. Prompt reporting will allow the organisation to assess the likely impact of the loss and take any mitigating action. Any delay may cause serious harm. If you lose or mislay Parliamentary information you must:

- report it immediately to your Line Manager
- follow the guidance and complete the information loss form which may be found at the following Intranet link:

Reporting loss or misuse of information

5.4 Depending on the circumstances and the severity of the incident it may be decided that other key personnel should be informed and an internal communications and media plan be established.

5.5 Failure to report loss or theft could result in disciplinary procedures being taken against you.

Your responsibilities

5.6 You must:

- understand your responsibilities to protect information
- ensure that personal and sensitive Parliamentary information is protected by appropriate security to guard against its loss or inappropriate disclosure both on and away from the parliamentary estate
- respect the rights of people to access information in a way provided for by the law
- report breaches and information losses promptly to your Line Manager
- make sure that information is not misused
- take particular care in protecting sensitive information
- ensure that information is used correctly and shared with the right people
- discuss with your Line Manager if you are unclear as to what action is necessary to keep information secure, or if you are in any doubt about how you should deal with certain personal or business sensitive information
- choose a secure, strong password on your PC
- only use Parliamentary Digital Service-supplied encrypted memory sticks for Parliamentary information
- keep all portable devices (mobile phones, laptops, tablets, memory sticks) safe at all times and always protect these with a password or pin number as appropriate
- regularly attach your Parliamentary laptop to the network in order to receive the latest security updates
- lock your work station using Ctrl-Alt-Delete Return, even if you are away for only a few moments
- shred or arrange for secure disposal of sensitive information
- clear sensitive information from your desk at the end of the day
- lock filing cabinets containing sensitive hard copy information outside business hours and when rooms are left empty during the day
- ensure keys to cabinets which contain sensitive information are securely stored outside business hours, preferably in a combination key safe
- ACT FAST and report any information loss, hard copy or electronic, or breach to your Line Manager and follow the relevant procedure as a matter of urgency
- always use the Protective Marking Scheme where required
- ensure you are familiar with the policies and procedures outlined in this chapter and in the Parliamentary ICT Security Policy which may be found on the following Intranet link:

Security Policies and Advice

5.7 Managers must:

- take all reasonable steps to ensure that information concerning security procedures are provided to your staff, including contractors and non-permanent staff permitted access to personal and business sensitive Parliamentary information
- report any information breaches or risks
- ensure system access rights are updated or removed when a member of staff moves or leaves
- ensure that the Parliamentary pass is collected and the Pass Office notified when a staff member leaves

5.8 You MUST NOT:

- take sensitive Parliamentary information, hard copy or electronic, off the Parliamentary Estate without first receiving the authority of your Line Manager
- talk about confidential information to anyone outside the House or pass it on to anyone outside the House unless authorised to do so. Such authority may arise as part of your employment with the House of Commons Service or from an express instruction by your Line Manager. You must continue to keep such information confidential even after your employment with the House of Commons Service has ended.
- share your password
- read or display sensitive information in public places or transport it in see-through folders or wallets
- forward sensitive information to your personal or internet email accounts
- use non-Parliamentary Digital Service memory sticks or non-encrypted laptops to transport sensitive electronic information off the estate
- download unapproved or unlicensed software on to your Parliamentary computer
- leave sensitive information in view on your desk
- store Parliamentary information on personal devices

6. Where to Go for Help or Further Advice

6.1 You can get further advice and help from:

The IRIS Service

The IRIS Service is working to help you make the right decisions about processing, protecting and disclosing information and data you are required to work on. Privacy, confidentiality, integrity and accessibility are the fundamental principles of the work of the IRIS service.

SIRO/DIRO

Senior Information Risk Officer (SIRO)

The SIRO is the senior person responsible for overall information assurance for the House of Commons Service at The Board level. The Managing Director of Information and Research is the SIRO.

Departmental Information Risk Officer (DIRO)

Each Team has a designated DIRO. The DIRO is the senior person in each Team with overall responsibility for information risk assessment, monitoring and mitigation. They will provide assurance to their Managing Director and to the SIRO that risks have been identified and addressed and that business practices accord with policies and guidance.

A list of DIROs can be found at the following Intranet link:

List of Departmental Information Risk Owners

Return to the Staff Handbook.