Chapter 22: The Parliamentary Network

1. About this Chapter

1.1 This chapter explains the principles and procedures for using the Parliamentary network and the rules governing the following:

- procedures in place to ensure privacy of data
- data storage and disposal
- computer viruses
- treatment of computer
- computer monitoring
- use of the Internet
- use of social networking sites (including Twitter)
- Your responsibilities when using the network to ensure data security.

2. Principles

2.1 It is every computer user's responsibility to ensure the confidentiality, integrity and availability of data stored on computers and to use computers in a proper manner. Following the procedures set out below will help you to fulfil this responsibility. These procedures are the basic minimum and there may be stricter procedures operating locally.

2.2 Remember that computers are supplied for business use. Any personal use should be incidental. Unauthorised access to any Parliamentary or external system is prohibited. Any non-compliance with this policy may lead to disciplinary action being taken against you.

2.3 All staff should read and be aware of the Parliamentary ICT Security Policy, which is at Annex A and on the Intranet at:

Security Policies and Advice

3. Procedures

3.1 To ensure the privacy of data and to prevent unauthorised users gaining access to systems, you should log-in to the Parliamentary network. Confidential documents should be password protected.

3.2 Passwords must follow Parliamentary Digital Service guidance:

- minimum of eight characters, including upper and lower case letters and a number and/or symbol
- must not be based upon easily guessed words or obvious attributes, such as addresses, telephone numbers and car registration numbers
- must be changed on other systems according to local guidelines

- Ideally should not be written down unless absolutely necessary, for instance if you have to use multiple passwords. If you do have to write passwords down the information must be kept secure in a locked drawer or cabinet.
- Should not be disclosed to others. If you have to reveal your password to the Parliamentary Digital Service's service desk or to the Parliamentary Digital Service to enable them to reconfigure your computer or account, change your password immediately afterwards.

Absences from your desk

3.3 To prevent unauthorised access to your systems you should lock your workstation when you intend to be away from your desk (use the Windows symbol key plus L to lock/unlock). All machines will automatically lock after a fixed period, but you should not rely on this when leaving your desk.

Data storage and disposal

3.4 Data stored on your PC's hard disk are not backed-up and are vulnerable to corruption and/or loss. All business documents should be saved to the appropriate parts of the SPIRE system or team network fileshares in limited cases. Otherwise, you should seek guidance from the Parliamentary Digital Service's service desk on ext. 2001 if you have a specific requirement to store sensitive information.

3.5 Only work-related data should be stored on the network. Your personal fileshare is provided primarily for the temporary storage of files to which you wish to restrict access, such as staff performance, your own HR records, or other sensitive material.

4. Removing Parliamentary Data from the Estate

4.1 You must not remove Parliamentary data from the Estate unless authorised to do so by your Line Manager and/or your Information Risk Officer.

4.2 Where it is necessary to remove sensitive electronic data from the Estate and permission to do so has been obtained, only encrypted laptops or encrypted USB memory sticks provided by the Parliamentary Digital Service should be used). Standard mobile phones should always be protected with a password or pin number.

4.3 Storing or transporting sensitive Parliamentary data to the Parliamentary Estate work or away from the Parliamentary Estate should be the exception rather than the rule. Managers are expected to consider the scope to rearrange existing duties to allow staff to work on sensitive data within the secure environment of the estate in the first instance. Authority to remove data and work on it away from the Parliamentary Estate should be given only where there is a clear business need to do so and where steps have been taken to minimise risks or mitigate the impact of loss or breach.

4.4 You should also be aware of the Parliamentary ICT Security Policy concerning the use of personal email accounts for processing Parliamentary data. The policy is available on the Intranet at:

Security Policies and Advice

4.5 Authorisation from your Line Manager 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.

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

Tips for safer remote working (PDF 65 KB)

5. Viruses

5.1 Viruses and other malicious software programs have the potential to cause many problems, including corrupting or stealing your data. As a rule:

- never load anything onto your computer without virus checking first
- never download programs from the Internet
- always virus check portable media such as USB sticks, CDs, or DVDs before use
- Do not attach personal, or free, USB sticks (sometimes given out at events) to Parliamentary computers.

5.2 If you suspect that your computer has become infected with viruses or malware you should immediately contact the Parliamentary Digital Service's service desk on ext. 2001.

5.3 If you have any questions about the information above or need assistance with virus checking, you should contact the Parliamentary Digital Service's service desk on ext. 2001.

6. Treatment of Computers

6.1 Computers and related equipment should be used in a responsible manner and respected as complex tools and treated with care. As a rule:

- do not load software without the knowledge and assistance of the Parliamentary Digital Service, as this may corrupt your set-up
- do not pirate software or use any unlicensed copies
- do not drink or eat too close to the computer keyboard (coffee and crumbs do not mix well with electrical equipment)
- keep laptop computers under lock and key when not in use

7. Email

Statement on monitoring

7.1 At the discretion of a Team's Managing Director or Head of Office, Business Management Director or their equivalent, the House reserves the right to monitor incoming and outgoing emails, and other use of the Parliamentary network including access to the

Internet and social networking sites, to establish that the system is being used properly for necessary and lawful purposes.

7.2 Any access or monitoring will be conducted in accordance with the requirements of the Data Protection Act 1998, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699, and the Regulation of Investigatory Powers Act 2000. The Parliamentary network may apply automatic message monitoring, filtering, and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of the Parliamentary ICT Policy.

Email use

7.3 At the discretion of a Managing Director or Head of Office, or Business Management Director, emails may be reviewed for the purpose of responding to requests for disclosure under legislation such as the Data Protection Act, the Freedom of Information Act or the Environmental Information Regulations 2004. When writing emails you must be aware that they form part of the official business record and that the House may be required to disclose their content in response to a request and as part of evidence for formal proceedings such as Employment Tribunals.

7.4 You are permitted to make occasional personal use of the email system provided that this does not interfere with the performance of your normal duties. However, the House authorities reserve the right to monitor emails, so privacy cannot be guaranteed (see the statement on monitoring at paragraphs 7.1 and 7.2). You must not:

- send or distribute email messages, attachments or other material which employ language or contain images that may reasonably be considered to be discriminatory, obscene, derogatory, offensive, threatening, insulting, illegal, harassing or harmful to recipients
- originate or distribute chain letters via email

7.5 If you receive a malicious or threatening email from any source you should inform your Line Manager immediately.

7.6 If you receive what you consider to be an inappropriate internal email you should forward a brief note to the sender explaining that you do not wish to receive any further emails of that nature. If the sending of inappropriate emails continues you should advise your Line Manager immediately.

7.7 If you receive an inappropriate email from outside the House of Commons which falls into the category of Spam, move the item to the HOP Spam samples folder in Outlook public folders. This will assist in blocking future occurrences.

7.8 Always be aware that unsolicited emails may contain malware or enable malware to be downloaded to your computer. Never open attachments or follow links in emails unless you are sure about the sender of the message.

7.9 If you intend to be away from the office for any length of time, remember to use the Out of Office Assistant (MS Outlook) to inform people that you are away. Please remember to include details of how long you will be away and who will be dealing with your work in your

absence. If you are away unexpectedly, your Line Manager may contact the Parliamentary Digital Service's service desk to activate your Out of Office Assistant with an appropriate message.

7.10 Any non-compliance with this policy on the use of the email system may lead to the application of the House of Commons disciplinary procedure (see chapter 20), which in serious cases could lead to your dismissal.

8. Internet Use

8.1 You are permitted to make occasional personal use of the Internet provided that this does not interfere with the performance of your normal duties. You should understand that the House may monitor your use of the Internet (see the statement on monitoring at paragraphs 7.1 and 7.2).

8.2 When using the Internet DO NOT:

- use it for any illegal purposes
- download information or pictures which are likely to cause offence to any other potential observers unless you have to do so in the proper discharge of your duties
- use the Internet for commercial activities, except in connection with your official duties

8.3 You must not deliberately visit websites or disseminate or retrieve information or software which contains material of an offensive, obscene or discriminatory nature.

8.4 In the event that you inadvertently access an inappropriate Internet site (as described above) you should immediately use the ‘Back’ button on the browser to return to the previous page or the ‘Home’ button to return to the Parliamentary Intranet home page.

8.5 The Parliamentary Digital Service blocks access to websites which potentially constitute a threat to the Parliamentary network and its users. If it is necessary for you to access such a website in the course of your duties, you should contact the Parliamentary Digital Service's service desk on ext. 2001 for advice on the possibility of obtaining a temporary easement.

Disciplinary sanctions

8.6 As a guide to Line Managers and staff, the policies on conduct and disciplinary procedures are set out in chapter 18 and chapter 20. However, listed below are examples of unacceptable behaviour relating to computer usage and the levels of misconduct that may be considered:

- excessive use of the email and Internet systems for personal, social or recreational reasons during work time could be classed as misconduct
- circulation of material of an offensive or discriminatory nature could be classed as serious misconduct
- circulation or retrieval of obscene material or the visiting of web sites which contain such material could be classed as gross misconduct

8.7 This policy also applies when accessing the Parliamentary network via a remote link.

9. Use of Social Networking Websites

9.1 The Social Media policy outlines the standards we require you to observe when using social media, the circumstances in which we will monitor the use of social media and the action we will take in respect of breaches of the policy. The policy should be read in conjunction with the Framework for Social Media

9.2 You are required to comply with the Social Media Policy in relation to any social networking sites that you use Any inappropriate use of social media may lead to the application of the House of Commons disciplinary procedure (see chapter 20), which in serious cases could lead to your dismissal.

10. Use of Parliamentary Instant Messaging

10.1 Instant messaging is another way of communicating in an easy and efficient manner with people around Parliament. It enables you to instantly text an individual or group of people and allows you to see the individual's availability or presence at the touch of a button. It also integrates with Microsoft Office and Outlook.

10.2 The use of instant messaging for social conversations should be kept to a minimum and should not interfere with the performance of your normal duties. Your instant messaging conversation is not saved, archived or journaled. Once your conversation is over, it is deleted from the system. You should use more appropriate methods, such as email and written documents, if you wish to save, archive or journal a conversation in accordance with the records management policy.

10.3 You should also be aware of the bicameral Parliamentary Records Management policy (see chapter 24). In general, instant messaging is well suited to ephemeral conversations, but should not be used for making formal decisions. It should not be used to:

- approve financial transactions
- enter into binding agreements with third parties
- enter into internal commitment for resources
- direct or approve official work to or from others
- attach files to the conversation
- send links to files held on the network
- communicate information that you would not want others to read

10.4 You must not send, formulate or distribute any material which employs language or contains images that may reasonably be considered to be:

- discriminatory
- obscene
- derogatory
- offensive
- threatening
- insulting

- illegal
- harassing
- harmful to the recipients
- in breach of the Data Protection Act 1998

10.5 The House of Commons Data Protection Act policy is on the Intranet at:

Data Protection

10.6 Any non-compliance with this policy on the use of the instant messaging may lead to the application of the House of Commons disciplinary procedure (see chapter 20), which in serious cases could lead to your dismissal.

10.7 If you receive what you consider to be an inappropriate message, you should forward a brief note to the sender explaining that you do not wish to receive any further messages of that nature. If the sending of inappropriate messages continues you should not close the conversation window, and you should advise your Line Manager immediately.

10.8 Instant messaging must only be accessed via your personal user account and you must not attempt to use another user's accounts. The instant messaging environment will not provide archive or journal functions, you should not rely on the Parliamentary Digital Service being able to obtain any historical correspondence as none will be kept.

10.9 You should not use instant messaging to disseminate long pieces of information as more appropriate media are in place to address this type of communication, for example, emails.

11. Further Advice

11.1 If you have any queries about computer use, contact the Parliamentary Digital Service on ext. 2001 or the Parliamentary Digital Service training team on ext. 8284. If you require specialist advice or guidance, please contact the Parliamentary Digital Service Security & Risk Manager on ext. 4455.