Chapter 22: Parliamentary Digital Services

1. About this Chapter

1.1 This chapter introduces key principles for using parliamentary digital services and explains a number of important topics of which users should be aware, including the following:

- security of data
- data storage
- computer viruses
- treatment of devices including computers, tablets and smartphones
- computer monitoring
- use of the Internet
- use of social media

2. Key Messages

2.1 It is the responsibility of all staff to use devices in a proper manner and to ensure the security of parliamentary data and information. Following the guidance and direction set out below will help you to fulfil this responsibility. The detail provided in this chapter is the basic minimum and there may be stricter procedures applicable to you operating locally.

2.2 Remember that devices 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 Parliamentary Digital Service’s security policies, procedures or other supporting security documentation may lead to disciplinary action being taken against you.

2.3 All staff should be aware of the parliamentary security policies and are required to pay particular attention to Acceptable Use – User Responsibilities available on the Intranet at Policies and Procedures for House of Commons and Digital Service staff.

3. Security of Data

3.1 Access to your parliamentary account is controlled using multifactor authentication, which includes your password. You are responsible for your account and must follow Parliamentary Digital Service guidance on managing your login credentials. Key messages on protecting your password are below and you should read Password Management – User Responsibilities (PDF 598 KB). More information is also available on the Intranet:

**Passwords**

- don’t share your password with anybody. You will not be asked to share your password with any person or team, including the Digital Services Helpdesk
- change your password if you suspect it has been compromised.

3.2 Remember to use passwords and/or PINs on tablets and mobile phones.
3.3 Some information, including personal data, may be particularly sensitive. You should consider using password protection for documents containing sensitive information.

**Absences from your desk**

3.4 To prevent unauthorised access to your account you should lock your screen when you leave your desk. A quick way to lock your screen if you are using a computer with Windows is to press [Windows key] and [L] at the same time, or [Ctrl]+[Alt]+[Delete] followed by [Return].

**Data storage**

3.5 Data stored on your device is not backed-up and is vulnerable to corruption and/or loss. All business documents should be saved to protected online storage locations such as SharePoint and OneDrive. Otherwise, you should seek guidance from the Parliamentary Digital Service Support Desk on ext. 2001 if you have a specific requirement to store sensitive information.

3.6 Minimal amounts of personal data may be stored on parliamentary systems but this is at your own risk (the Digital Service is not responsible for the loss of personal/private information stored on parliamentary systems) and provided it does not contravene any parliamentary policies, rules or instructions, or any applicable legislation.

4. Removing Parliamentary Data from the Estate

4.1 You must not remove parliamentary data from the Parliamentary Estate unless authorised to do so by your Line Manager and/or your Information Risk Officer. This includes the capability provided by Office 365 to synchronise digital information with your parliamentary and personal devices and exported digital information on removable media (e.g. USB memory sticks). You should not synchronise to personal devices (laptops and desktops). In line with our current guidance and policy around information security (see [Chapter 23](#)), you may be subject to disciplinary action should evidence of OneDrive Sync Client downloads on personal devices come to light.

4.2 Where it is absolutely necessary to remove sensitive electronic data from the parliamentary estate and permission to do so has been obtained, only encrypted laptops or encrypted media (e.g. CD/DVD/USB memory sticks) provided by the Parliamentary Digital Service should be used.

4.3 Storing or transporting sensitive hard copy parliamentary data to 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.

Further tips and best practice on working remotely and safeguarding information are available on the Intranet at the following links:

[Tips for safer remote working](#) [Working on or off the Parliamentary Estate](#) [Your role in safeguarding information](#)
4.4 Parliamentary information must not be automatically forwarded to your personal email account. More detail on email can be found on the Intranet at:

Acceptable Use of Parliamentary Digital Services – User Responsibilities

Cyber Security

4.5 If you do need to forward non-public parliamentary information to a personal email account or use externally provided services for the production and/or storage of official data or documentation, then seek authorisation from your Line Manager beforehand. You should also be aware of the Parliamentary Protective Marking Scheme. (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:

- always virus check portable media such as USB memory sticks, CDs, or DVDs before use
- never import anything onto your device without first checking it for viruses
- contact the Digital Service Support Desk on ext. 2001 if you suspect you have a computer virus or if you have reason to believe your anti-virus software is not working.

5.2 If you have any questions about the information above or need assistance with virus checking, you should contact the Digital Service Support Desk on ext. 2001.

6. Treatment of Computers, Tablets and Smartphones

6.1 Computers, tablets and smartphones are commonplace but you may use other devices in your work within Parliament. All equipment and devices should be used in a responsible manner, respected as complex tools and treated with care. Key messages when using computers, tablets and smartphones are below:

- don’t try to install or uninstall software on your parliamentary devices without authorisation from the Digital Service Support Desk. All software must be licensed and used in accordance with current legislation
- don’t connect unauthorised USB devices to your device
- remember to keep food and drink away from computers
- treat your devices as if they were a large amount of cash – keep them under lock and key when not in use
- all users should complete the relevant online Cyber Security Awareness Module and familiarise themselves with Acceptable Use of Parliamentary Digital Services – User Responsibilities.

6.2 If you lose or damage your equipment you must report this to the Digital Support Desk (x2001) immediately. The process can be viewed on the Computer Policy and Guidance intranet page. Repeat damage or loss of official equipment will be reviewed and may be escalated where appropriate.

7. Email

Statement on monitoring
7.1 In common with many organisations, protective monitoring (a log of activity) is performed on the digital services you use, which includes email and other Internet activity (e.g. web browsing). This routine monitoring, for example email filtering and web blocking services, is required to protect parliamentary systems and to establish that systems are being used lawfully and in accordance with security policies. Exceptionally, and at the request of an investigating manager with the approval of a Team’s Managing Director or Head of Office, Business Management Director or their equivalent, the House reserves the right to access and review an employee’s email account and other use of the parliamentary network. This non-routine measure will usually be as part of a disciplinary investigation where there are grounds to suspect misconduct (including misconduct unrelated to use of the parliamentary network) may have occurred. Staff should mark any personal emails or correspondence with Trades Unions as such and encourage those who send them to do the same. The House will avoid, where possible, opening emails clearly marked as private or personal.


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 access and monitor emails, so privacy cannot be guaranteed (see the statement on monitoring at paragraphs 7.1 and 7.2).

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

7.6 If you are concerned about an email from outside the House of Commons, or think you may have clicked on a suspicious link or attachment, please report it immediately to the Digital Service Support Desk by calling ext. 2001.

7.7 Always be aware that unsolicited emails may contain malware (e.g. computer viruses) 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.

7.8 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 Helpdesk to activate your Out of Office Assistant with an appropriate message.
7.9 Any misuse of email 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 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 Digital Service Support Desk on ext. 2001 for advice on the possibility of obtaining a temporary easement.

8.3 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
- 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 web site 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 Any misuse of the Internet may lead to the application of the House of Commons disciplinary procedure (see chapter 20) which in serious cases could lead to your dismissal.

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 (which also includes in section 9 examples of unacceptable behaviour relating to computer usage and the levels of misconduct that may be considered).

8.7 Disciplinary sanctions also apply when accessing parliamentary digital services via a remote link.

9. Use of Social Media

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 (e.g. Skype for Business and Microsoft Teams) is another way of communicating in an easy and efficient manner with people around Parliament. It enables you to
instantly message 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 only retained for twenty-four hours after which time the conversation is deleted. It 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 Information and Records Management policy.

10.3 You should also be aware of the bicameral Information and Records Management policy (see chapter 24). In general, instant messaging is well suited to brief 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
- 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 2018

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, email.

11. Further Advice

11.1 If you have any queries about computer use, contact the Digital Service Support Desk on ext. 2001. If you require specialist advice or guidance, please contact the Parliamentary Digital Service Cyber Security Team on ext. 4455.

Return to the Staff Handbook.