Use of departmental resources policy

- Status: Current policy
- Applies to: Home Office
- Issued: July 2008
- Updated: March 2013

In brief

You must use official resources appropriately and in line with the rules and standards set out by the department.

Principles

1) All members of staff must adhere to the rules regarding departmental resources and operate them with maximum efficiency. Inappropriate use of any Home Office or Crown resource, such as IT or postage, could be a disciplinary offence.

2) This policy applies to the use of:

- internet
- email
- telephone
- mobile phones
- fax machines
- official stationery
- private correspondence
- trading activities

What it means in practice

3) You must not make inappropriate use of the official time, information and resources, either of the department or of the Crown. Such inappropriate use may constitute a disciplinary offence. You should adhere to IT security guidance.

Related links

HR and learning

- Grievance resolution
- Guidance on using social media at work
- IT systems security
- Use of departmental resources policy - Annex A
- Use of departmental resources policy - Annex B
- Use of departmental resources policy - Annex C
- Use of departmental resources policy - Annex D
- Use of departmental resources policy - Annex E

IT services

- IT policy and security for staff

Adelphi services

- Shared service centre support

External links

- Information Commissioner's Office

Internet

4) The internet is a business tool and you should treat it in the same manner as any other departmental resource. You are able to make reasonable use of the internet in the workplace, for personal reasons; however, this must not interfere with the work of the Home Office. Your personal use of the internet, or any other IT system, must not interfere with or take priority over your work responsibilities.

5) You are allowed to access the internet for personal use before starting work in the morning, once work has finished in the evening (with the permission of your line manager), or during a lunch break or any other formally recognised break. If you do not have a specified lunch break, use during the working day is permitted for limited periods. You must not use the internet for personal purposes outside these times, unless there is an emergency and your line manager agrees that it warrants the use of the internet.

6) You should be aware that the internet is not a secure medium and that there are risks when supplying any personal details; principally, this applies to using links that have not been encrypted.

7) You are responsible for ensuring that any information you supply on the internet will not result in legal action being taken against you or the Home Office; the laws of contract, defamation, copyright, harassment, obscenity and confidentiality apply to internet communication in the same way as they apply to traditional ways of communicating.

8) You should not download or circulate any material that could introduce a virus into the system or that could compromise data; if you are found to have introduced or circulated such material, you will be liable to disciplinary action. If the circumstances are serious, criminal prosecution could result.

9) You should report suspected internet misuse to a line manager. All managers must take appropriate action when employees are found to be misusing the system.

10) If you are required, as part of your official duties, to research specialist internet sites which are deemed inappropriate, you should use a standalone computer, and you must get the prior agreement of a member of the senior civil service. You must also retain a clear audit trail detailing why you carried out the research and you must show that you assessed the risk of negative publicity or embarrassment.

Email

11) You can make reasonable use of email for personal reasons as long as it does not interfere with:

- the work of the Home Office
- the performance of your duties
- other employees carrying out their work
- the effective operation of the email system

12) Unacceptable use of email could result in your facing disciplinary action.

13) You should be aware, when using email for business purposes, that it has the same authority as any other business communication. You should not include anything in email communication that you are unable to account for or would not be willing to disclose; emails are classed as published information and, under the Data Protection Act 1998 and the Freedom of Information Act 2000, all forms of documents, including email, are potentially disclosable and may be admissible as evidence in a dispute.

14) You must be aware that email can also inadvertently create a binding contract; any inaccurate or misleading statement about Home Office services (whether deliberate or accidental) can lead to legal claims of misrepresentation.

15) You must ensure that any email you send is not in breach of the law. Employees are legally bound not to send any email that includes:

- potentially libellous remarks made about a fellow employee or an external customer
- the accidental formation of contracts where a customer relies on information given
- defamation
- copyright infringement and computer misuse
- material that is inflammatory, sexually explicit, sexist, racist, homophobic, or religiously offensive in content and capable of amounting to harassment (as outlined in the resolution [staff complaints] policy and guidance).

16) Sending or forwarding emails that contain abusive, sexually inappropriate or explicit, obscene, illegal, offensive or defamatory material is a disciplinary offence. You must inform your line manager immediately if you receive an email from a work colleague containing such content. You must inform the relevant IT security unit if the email has been sent from an outside source. Failure to report is a disciplinary offence.

Monitoring of internet and email

17) The Home Office reserves the right to intercept emails and to monitor internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, for the following reasons:

- to ascertain compliance with regulatory or self-regulatory practices, or procedures relevant to the business
- to detect or prevent crime
- to maintain an adequate level of security for Home Office computer systems
- to detect any computer viruses
- to check an employee's emails during long-term absence to ensure that business emails are actioned, thereby maintaining business continuity
- to support capacity planning, compliance with service levels, etc, and
- to detect misuse of any official equipment

18) The computer system automatically logs internet access and emails on a 24-hour basis, including the actual times that an individual uses it. No matter when the facilities are used, the same standards of conduct apply and the same action will be taken if they appear to have been used inappropriately.

19) Personal emails will be opened only in exceptional circumstances; for example, where there are grounds to suspect potential criminal activity or harassment of other people.

20) In exercising its right to monitor emails and internet usage, the Home Office is conscious of its obligations under the Data Protection Act 1998, as information derived from the interception of communications is covered by the data protection principles. Further information can be found on the Information Commissioner's Office website.

21) You may face criminal prosecution and disciplinary action if monitoring reveals:

- unauthorised use
- any serious or repeated breach of this policy, or
- any other form of use that is potentially damaging to the Home Office

22) Line managers should be aware that, although the usual route by which abuse comes to light is through monitoring by the system provider, primary responsibility lies with line management. If investigation of any particular incident were to produce clear evidence that managers have ignored persistent abuse, they themselves would become liable to disciplinary action.

Telephone and work mobile phones

23) You are permitted to reasonable occasional use of office telephones to make personal calls providing that the calls are kept to a reasonable length of time and to local and national landline numbers and UK mobile phones only. You should also keep personal incoming calls to a reasonable length. The making and receipt of personal calls using office telephones should not interfere with or cause disruption to work responsibilities and is always subject to the needs of the business. You must seek agreement from your line manager if there is a need to use an office telephone for an extended period of time.

24) You must not use official telephones to call international numbers or premium rate numbers.

25) You must not accept incoming reverse charge calls unless you have obtained agreement from your line manager.

26) Telephone monitoring, other than the normal quality assurance process – for example, in call centres – will only occur as part of an official investigation where there are specific grounds for doing so. The agreement of the departmental security unit or, in the former UK Border Agency, the security and anti-corruption unit, must be obtained before any such monitoring takes place.

Personal mobile phones

27) You should use your personal mobile phone courteously while in the office; you should switch it to silent and should keep conversations to a reasonable length.

Cameras

28) You must not use a camera (including a mobile phone camera) for personal use in any Home Office building unless you have prior permission from your line manager. The unauthorised taking of photographs is a security breach and may lead to your facing disciplinary action.

Fax machines

29) You must not send facsimiles (faxes) of a personal nature to international numbers from either a fax machine or a computer. If you wish to send a personal fax to a local or national number you should seek permission from your line manager.

Official stationery

30) You must not use official stationery, such as headed paper, for personal purposes, as this could be viewed as your trying to exploit your position as a Home Office employee to influence others for your own gain. Such use of official stationery could result in disciplinary action.

Official property

31) If you damage official papers or property, you must report this immediately through your line manager to your head of unit or equivalent. You are liable to pay any costs to replace or fix the damaged item.

Private correspondence

32) You should not use the address of any official premises to head any private correspondence, nor should you send private correspondence to any official premises; the department will not accept any liability for the loss of any private correspondence. If you are sending a personal letter from your work address, you should ensure that you have stamped the letter with the required postage stamps.

Trading activities

33) You must not use the department's premises, your official work address, your official time, or any official information or resources, to conduct any private trade or business, or to canvass or advertise for any such private trade or business.

Display of public notices

34) No notices of any kind may be exhibited on the premises of the department without official consent. Please refer to the instructions displayed on each notice board for guidance.

Policy annexes

- Annex A – Acceptable use of the internet
- Annex B – Unacceptable use of the internet
- Annex C – Unacceptable use of email
- Annex D – Good email etiquette
- Annex E – Internet, email and telephone policy: action to be taken

Further information and contact point

Please read carefully through the guidance on this page, along with any associated documents at related links.

If you still have any questions about this policy after doing so, contact the Home Office shared service centre (SSC) – see the related link, 'Shared service centre support'.

This version of the policy incorporates staff handbook chapter 3.