



## 2. Personal responsibility for safeguarding information

### Introduction

Regardless of how good our systems are in protecting our information, that information will be safeguarded effectively only if each individual takes the necessary steps to ensure that we look after it, particularly away from the office.

It is often very much due to individual carelessness that information is disclosed without authority or that it is found by persons who are not entitled to it. Even if the lost information is not sensitive, this can risk damaging the confidence that ministers and the public have that the department can safeguard information and do its job well.

Loss of information, particularly through carelessness, is something the department takes very seriously. The department is determined to ensure that everyone who works in the Home Office and its agencies is aware of just how important it is for them to safeguard the information in their trust; if information is lost there will be consequences both for the department and for the individual.

### Purpose of guidance

The purpose of guidance is to remind individuals of their personal responsibility for safeguarding against the loss or unauthorised disclosure of information (for example, that contained on hard and electronic copies of documents and in case files, laptops, memory sticks and BlackBerrys, and so on) and the possible consequences of failing to do this.

Responsibility for safe handling of official information rests with the person to whom it is entrusted. Documents (whether hard or electronic copies) must be marked at the appropriate level and protected accordingly (see the departmental security unit's 'Quick reference guide to handling protectively marked material' at Related Links). Regardless of whether it is protectively marked, official information must be handled with care to prevent it from being released to those who do not have the need to see it.

### Protecting information within the office

The Home Office operates a clear desk policy, subject to practicability, in some operational areas. When leaving the office, all documents and other information storage media must be locked up in appropriate containers.

Protectively marked material must be stored according to the guidelines for each level (see 'Quick reference guide to handling protectively marked material' at Related Links) and must never be left out in

## Related links

### Downloads

- > [Quick reference guide to handling protectively marked material](#)
- > [Secure remote working: a quick reference guide](#)
- > [Security compliance officers](#)

### Work tools and guides

- > [Information assurance and security](#)

### HR and learning

- > [1. Security management and roles](#)
- > [Frequently asked questions about your personal responsibility for safeguarding information](#)
- > [Use and misuse of official information policy](#)

unoccupied rooms. Documents should not be left on desks, photocopiers, printers or faxes.

### **Protecting information outside the office**

Should you need to take any official documents outside the office, you have a personal responsibility to ensure their security and you must take the utmost care of them. Even documents that are not protectively marked should be taken out of the office only where there is a genuine business need and must never be left unattended. They should also be carried in a way that ensures that they are hidden from view, preferably in a case or bag.

Taking sensitive, protectively marked documents outside the office represents the greatest risk. Such documents should not be taken outside the office unless it is absolutely essential for the conduct of our work and there is no more secure alternative for managing the transfer of the information.

You must obtain permission from your line manager to take protectively marked documents out of the office and, where appropriate, the security compliance officer (SCO) should be informed (information on the duties of the SCO, along with a list of SCOs is available under Related Links).

Protectively marked documents must be carried in strict accordance with published guidelines, which set out the exact requirements for conveying documents at each level of protective marking. All removable media must be encrypted to a Home Office-approved standard.

Utmost care must also be taken when reviewing any information in a public place, as this increases the risk that others, who are not authorised to do so, are able to view sensitive information. In busy places, it also increases the risk of valuable information sources (for example, on Blackberrys or laptops) being stolen or of papers being left behind. Protectively marked documents must never be reviewed or worked on in a public place.

### **What could happen to me if I failed to protect a document?**

#### **Within the office**

Depending on the circumstances, there is potential for disciplinary action being taken, which could result in a range of penalties up to and including dismissal. In certain limited circumstances, disclosure of information could constitute an offence under the Official Secrets Act 1989 (see 'Use and misuse of official information policy' at Related Links), resulting in criminal prosecution against you.

#### **Outside the office**

Your first priority should be to notify the department immediately so that action can be taken to recover the document and minimise any potential damage. Failure to do so will be taken very seriously.

Depending on the circumstances, you could incur a range of penalties. Disciplinary action could be taken up to and including dismissal, regardless of the consequences of the breach. In some circumstances, disclosure of information in this way could constitute an offence under the Official Secrets Act (1989) (see 'Use and misuse of official information policy' at Related Links). Failure to safeguard data could also constitute the common law criminal offence of misconduct in public office. In both cases, you could be subject to criminal prosecution.

The other pages in this section and in the 'Information assurance and security' section provide further guidance on protecting official information.

---

### Page Tools

[Add to my favourites](#)

---

---

### Rate this information

Current rating:  
★ (2 ratings)

My Rating:

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Poor [»](#) Good

[Rate it](#)

© Crown copyright

[Terms and conditions](#)

**Directgov**  
Public services all in one place



[info4local.gov.uk](http://info4local.gov.uk)

[homeoffice.gov.uk](http://homeoffice.gov.uk)