

Personal safety advice

Personal safety advice

About this guidance

Why personal safety advice is important General advice on protecting and giving out information Protecting personal information and safety - using computers Protecting personal information and safety - exposure to identity theft	<p>This guidance gives information to Home Office staff and criminal and financial investigators working in the enforcement and crime directorate. It gives an overview and advice on general matters that can impact upon your operational work.</p> <p>The guidance contains information on the following:</p> <ul style="list-style-type: none">• general personal safety advice• giving out information, and• protecting your personal information. <p>Changes to this guidance - tells you what has changed since previous versions of this guidance.</p> <p>Contact - tells you who to contact for help with a specific case if your manager can't answer your question.</p> <p>Information owner - This page tells you who the information owners are and tells you how the guidance can be updated.</p>	<p>In this section</p> <p>Changes to this guidance</p> <p>Contact</p> <p>Information owner</p>
---	---	---

Personal safety advice

Changes to this guidance

[About this guidance](#)

[Why personal safety advice is important](#)

[General advice on protecting and giving out information](#)

[Protecting personal information and safety - using computers](#)

[Protecting personal information and safety - exposure to identity theft](#)

This page lists changes to the personal safety advice guidance, with the most recent at the top.

Date of the change	Details of the change
26 July 2013	Six month review by the modernised guidance team: <ul style="list-style-type: none">• Minor housekeeping changes.
23 January 2013	Six month review by the modernised guidance team: <ul style="list-style-type: none">• Contact:<ul style="list-style-type: none">○ restricted information has been changed• Minor housekeeping and plain English changes.
	For previous changes you will need to access the archived guidance. See related link: Personal safety advice - archive.

Related links

See also

[Contact](#)

[Information owner](#)

Links to staff intranet removed

Personal safety advice

Why personal safety advice is important

About this guidance Why personal safety advice is important General advice on protecting and giving out information Protecting personal information and safety - using computers Protecting personal information and safety - exposure to identity theft	<p>This page tells you why personal safety is important and how the department and you can protect your identity and reduce criminal efforts to target staff.</p> <p>Why you need to protect your safety</p> <p>If you work in the enforcement and crime group it can increase attention towards you from:</p> <ul style="list-style-type: none">• the media• suspects• staff• Home Office customers, and even• family members. <p>Conducting criminal investigation work means there is more chance you will come into contact with criminals. Some criminals will do anything to avoid arrest or having their business disrupted. Instances of staff being targeted are rare, but there is a structure in place to help support and protect staff.</p> <p>How the Home Office helps to protect staff</p> <p>The department has a number of ways to identify and give advice on security risks.</p> <table><tr><td>The enforcement and crime group (ECG).</td><td>There is a named operational security manager responsible for overall security in the crime directorate.</td></tr><tr><td>Each location (this may be a team or a building).</td><td>There is a local operational security manager responsible for:<ul style="list-style-type: none">• giving advice on operational work, and• identifying and reducing risks.</td></tr></table>	The enforcement and crime group (ECG).	There is a named operational security manager responsible for overall security in the crime directorate.	Each location (this may be a team or a building).	There is a local operational security manager responsible for: <ul style="list-style-type: none">• giving advice on operational work, and• identifying and reducing risks.	Links to staff intranet removed
The enforcement and crime group (ECG).	There is a named operational security manager responsible for overall security in the crime directorate.					
Each location (this may be a team or a building).	There is a local operational security manager responsible for: <ul style="list-style-type: none">• giving advice on operational work, and• identifying and reducing risks.					

	The security and anti-corruption unit (SACU).	They work to highlight risks to the department and staff. To contact SACU, please see related link: Security contacts.	
	<p>How you can protect yourself</p> <p>You must be aware of any increased risks because of the work you do.</p> <p>There are various ways you can reduce potential risks to yourself. This personal safety guidance tells you some of the ways that you can reduce possible risks. You must discuss personal and operational safety with:</p> <ul style="list-style-type: none">• your line manager• the operational security officer network, or• SACU.		

Personal safety advice

General advice on protecting and giving out information

About this guidance Why personal safety advice is important General advice on protecting and giving out information Protecting personal information and safety - using computers Protecting personal information and safety - exposure to identity theft	<p>This page tells you about protecting information that you have access to and how to handle giving out information.</p> <p>Discussing your work You have a duty to show personal discretion when talking about your work. You must only discuss your work with those who need to know and who are authorised to have the information.</p> <p>You must never discuss specific cases with friends or family or anyone else who does not have that authorisation.</p> <p>Mandatory training on protecting information You must do the mandatory information management e-learning package on Discover which tells you how to protect information. For more information on the e-learning, see related link: Discover e-learning.</p> <p>Protectively marked information You must follow departmental rules about confidentiality and valuable information. Make sure you read and understand the Home Office's guidance on protecting information. For more information, see related links:</p> <ul style="list-style-type: none">• Quick reference guide to handling protectively marked material (UK Border Agency), and• 10 golden rules for staff handling personal data. <p>Giving out information You must:</p> <ul style="list-style-type: none">• not give out, misuse or discuss information outside the department without lawful authorisation:<ul style="list-style-type: none">○ this includes information you get through your work for the Home Office	Links to staff intranet removed
--	---	---------------------------------

	<ul style="list-style-type: none"> • not comment on Home Office information already available to the public • not comment or respond online on behalf of the Home Office officially, unless authorised by: <ul style="list-style-type: none"> ○ a press officer, and ○ an assistant director • direct all media enquiries to the press office. <p>Home Office or customer information has been released by mistake If you, or anyone else, release information by mistake, tell your line manager immediately so they can take the appropriate action.</p> <p>Line managers must report the incident to the security and anti-corruption unit (SACU). For more information, see related link: Security contacts.</p>	
--	--	--

Personal safety advice

Protecting personal information and safety – using computers

<p>About this guidance</p> <p>Why personal safety advice is important</p> <p>General advice on protecting and giving out information</p> <p>Protecting personal information and safety - using computers</p> <p>Protecting personal information and safety - exposure to identity theft</p>	<p>This section tells you some ways of protecting either your personal information, or work related information, when using computer equipment or the internet.</p> <p>Laptops or removable storage equipment</p> <p>You may have been issued with a laptop or Blackberry to help you with your daily work. When you are issued with this equipment, you will also receive instructions on its use and security. You must follow these instructions.</p> <p>If you are using shared equipment, for example a laptop issued to a team, you must make yourself aware of, and comply with, the current Home Office instructions on information security. For more information on these instructions, see related links:</p> <ul style="list-style-type: none">• Staying safe online guidelines: using the internet and social media at home and work.• Get Safe Online, which is a public site involving:<ul style="list-style-type: none">○ the Home Office and other government departments○ sponsors from many businesses including eBay, HSBC and Microsoft, and○ supporters from numerous businesses such as Yahoo, MSN, Citizens Advice and Paypal. <p>Some other, more general advice to follow is:</p> <ul style="list-style-type: none">• Never leave the equipment unattended in a vehicle.• If you receive a new laptop or other equipment you must make sure the old one is:<ul style="list-style-type: none">○ returned, or○ disposed of properly.• Always 'password protect' or encrypt all information if you have private or departmental details on your equipment.<ul style="list-style-type: none">○ If you are using a group or shared password never write it down.• Never use the equipment in a public wireless hotspot.• If you are using a home wireless network:	<p>In this section</p> <p>Protecting personal information and safety - using social networks</p> <p>Links to staff intranet removed</p>
---	--	--

	<ul style="list-style-type: none">○ switch off this function when you are not using the equipment, and○ protect it with a higher level of security such as WPA or WPA2 (wi-fi protected encryption).● Do not carry information on a floppy disc or memory stick unless authorised. Keep these separately from your laptop.	
--	--	--

Personal safety advice

Protecting personal information and safety – using social networks

<p>About this guidance</p> <p>Why personal safety advice is important</p> <p>General advice on protecting and giving out information</p> <p>Protecting personal information and safety - using computers</p> <p>Protecting personal information and safety - exposure to identity theft</p>	<p>This page tells you some ways to protect your personal information and safety when using social networks.</p> <p>Social networking sites - personal use</p> <p>Social networking refers to social media sites, such as:</p> <ul style="list-style-type: none">• online discussion forums• blogs, and• social networking sites such as:<ul style="list-style-type: none">○ Facebook○ YouTube, and○ Twitter. <p>Although they are popular ways of communicating they can also present a threat to your:</p> <ul style="list-style-type: none">• privacy• personal information, and possibly• personal safety. <p>They can also carry risks to :</p> <ul style="list-style-type: none">• the Home Office• your colleagues, and potentially• our customers. <p>When using social media sites, it is up to you whether you tell people you work for the Home Office. You are recommended not to give this information but, if you do decide to, you must follow these additional instructions:</p> <ul style="list-style-type: none">• Do not post Home Office information on social networking sites unless you have	<p>In this section</p> <p>Protecting personal information and safety - using computers</p> <p>Links to staff intranet removed</p>
---	--	--

specific permission to do so. Laws of libel and other legislation that affect the Home Office apply to social networks and blogs as well.

- Never post customer or case information on social networking sites.
- Follow the same standards of conduct that you are expected to follow in other areas of your job.
- Never use your personal account to conduct Home Office work.

Using social networking sites as part of your work

You can be granted access to social networking sites if you need to use it as part of your work. This can only be authorised by a director after you have made a business case. You may:

- have limited access to the site, and
- not be able to use all functions.

Make yourself ‘a hard target’

Some websites and social media accounts are set up for malicious purposes and those who post online may not be who they appear to be. You must be aware that:

- Posting your personal details and location can leave you vulnerable.
- You may give out information about yourself without meaning to through the links you make with other people.
- Some social networking sites may share your information with third parties.

There are some simple steps that can be considered before using social media sites:

- Be careful about giving out information about you, your family and friends.
- Review you friends list regularly.
- Pay attention and know what is going on.
- Trust your instincts – if you have concerns about something you are probably right.
- Avoid confrontation.

For more information see related links:

- | | | |
|--|---|--|
| | <ul style="list-style-type: none">• Staying safe online guidelines: using the internet and social media at home and work,• Guidance on using social media at work. | |
|--|---|--|

Personal safety advice

Protecting personal information - exposure to identity theft

<p>About this guidance</p> <p>Why personal safety advice is important</p> <p>General advice on protecting and giving out information</p> <p>Protecting personal information and safety - using computers</p> <p>Protecting personal information and safety - exposure to identity theft</p>	<p>This page tells you about some ways to protect yourself against identity theft and how to protect your personal information.</p> <p>Your identity and personal information is valuable. Criminals can find out your details and use them to apply, in your name, for:</p> <ul style="list-style-type: none">• bank accounts• credit cards and loans• state benefits, and• documents such as passports and driving licences. <p>The Home Office and other public and private bodies contribute to a website that aims to fight the threat of identity theft and gives advice to people and organisations. For more information see related link: Action Fraud: Identity theft.</p> <p>Some of the key advice includes the following.</p> <ul style="list-style-type: none">• Keep your personal documents locked away in safe place at home. Consider storing valuable financial documents such as share certificates with your bank.• If your passport or driving license has been lost or stolen contact the issuing organisation immediately.• Never put in your bin:<ul style="list-style-type: none">○ bills or receipts○ bank statements, credit or debit card slips, or even○ unwanted post.• Destroy unwanted documents in a shredder. Identity thieves look through bins.• Check your statements when they arrive. If you see a transaction you don't recognise contact the company immediately.• Always know where your official identity passes are located and do not wear your Home Office pass or lanyard outside of work.	<p>In this section</p> <p>Protecting personal information and safety - your electoral roll details</p> <p>Protecting personal information and safety - your telephone directory details</p> <p>Protecting personal information and safety - your vehicle</p> <p>Links to staff intranet removed</p>
---	--	--

Personal safety advice

Protecting personal information – your electoral roll details

About this guidance Why personal safety advice is important General advice on protecting and giving out information Protecting personal information and safety - using computers Protecting personal information and safety - exposure to identity theft	<p>This page tells you about the different ways you can register your personal details on the electoral roll and what information you can restrict.</p> <p>The Representation of the People Act 1983 and the Electoral Administration Act 2006 set out the law on how UK residents must add their names to the Electoral Roll ('Register') in order to vote in local and national elections and referendums. You can register in three ways.</p> <p>Register in the full register This registration gives:</p> <ul style="list-style-type: none">• your name, date of birth and home address• details of whether you requested a postal vote and,• following an election, whether you voted. <p>These details can be accessed by certain people and government departments for specific reasons only.</p> <p>Register in the edited register In this register:</p> <ul style="list-style-type: none">• you can choose to include or remove your name and address and include only your eligibility to vote on the edited register, and• your name and address are replaced with a unique code, usually specific to the local authority area where you vote. <p>Anyone can purchase this register for any purpose and it is readily available on the internet.</p> <p>Total anonymous registration You can ask your local authority, in certain circumstances, how to be removed from the edited register so that none of your details appear. This can potentially affect your credit</p>	<p>In this section</p> <p>Protecting personal information and safety - your telephone directory details</p> <p>Protecting personal information and safety - your vehicle</p> <p>Links to staff intranet removed</p>
--	---	--

	<p>rating if you apply for a loan or mortgage.</p> <p>For more information see external links:</p> <ul style="list-style-type: none">• Representation of the People Act 1983• Electoral Administration Act 2006.	
--	---	--

Personal safety advice

Protecting personal information – your telephone directory details

About this guidance Why personal safety advice is important General advice on protecting and giving out information Protecting personal information and safety - using computers Protecting personal information and safety - exposure to identity theft	<p>This page tells you about protecting your personal information in telephone directories and how you can restrict the information they make available to the public.</p> <p>Directory entries</p> <p>If you have a home telephone or personal mobile phone the phone providers ask you to register or subscribe so that they can include your details in a directory showing your number, name and address. This is optional and you must consider if you want this information to be made publicly available. If your details already appear in a directory you can contact the supplier and ask them to remove your details.</p> <p>Withholding your number</p> <p>If you are a BT customer you can withhold your phone number when you dial other numbers. You do this by entering the code '141' before dialing the outgoing number. You can also set up with BT for this service to cover all outgoing calls.</p> <p>Protecting mobile phones</p> <p>You must protect mobile phones, particularly those issued for official business, with a personal identification number (PIN). If you have a phone with 'bluetooth technology' it must be password protected. You can opt to withhold your caller identity using the call options and bluetooth menus.</p> <p>If you are working on operational duties such as conducting surveillance must always disable the bluetooth mode before taking your mobile phone(s) with you on this work.</p>	<p>In this section</p> <p>Protecting personal information and safety - your electoral roll details</p> <p>Protecting personal information and safety - your vehicle</p>
--	---	--

Personal safety advice

Protecting personal information – your vehicle

About this guidance Why personal safety advice is important General advice on protecting and giving out information Protecting personal information and safety - using computers Protecting personal information and safety - exposure to identity theft	<p>This page tells you about what personal information is held in relation to your vehicle and how you can remove details to protect your personal details and safety.</p> <p>Driver and Vehicle Licensing Agency (DVLA) registration</p> <p>Your car registration is recorded on the main DVLA database. Anyone can purchase these details which include who a car is registered to, and at what address. It is possible to remove your details in certain circumstances and have your car placed on the DVLA blocking scheme.</p> <p>The operational security manager will advise you on whether you can justify removing your details. Any removal must be authorised by a grade 7 manager. It is sometimes possible to register your car to your office address instead of your home address.</p> <p>General personal security for your vehicle</p> <p>Some other, more general security advice for your vehicle:</p> <ul style="list-style-type: none">• Never leave your V5 vehicle registration certificate, MOT or insurance certificate in your car.• Remove dealer stickers from your rear window and number plate.• Do not renew the tax disc at your local post office as this will have a location stamp on it.• Remove, for example, local newspapers, train tickets, parking vouchers, receipts, bills, especially if you are using your own car on official business.• Make sure that your registration number is not attached to your vehicle keys.	<p>In this section</p> <p>Protecting personal information and safety - your electoral roll details</p> <p>Protecting personal information and safety - your telephone directory details</p>
--	--	--

Personal safety advice

Contact

About this guidance Why personal safety advice is important General advice on protecting and giving out information Protecting personal information and safety - using computers Protecting personal information and safety - exposure to identity theft	<p>This page explains who to contact if you need more help with a question about operational safety policy and guidance.</p> <p>If you have read this guidance and still need more help, you must first ask your line manager.</p> <p>If you need further help you may contact:</p> <div><div>Restricted - do not disclose – start of section</div><div>The information in this page has been removed as it is restricted for internal Home Office use only.</div><div>Restricted – do not disclose – end of section</div></div> <p>Changes to this guidance can only be made by the modernised guidance team. If you think the policy content needs amending you must contact the policy team, using the related link: CI inbox, who will ask the modernised guidance team (MGT) to update the guidance, if appropriate.</p> <p>The MGT will accept direct feedback on broken links, missing information or the format, style and navigability of this guidance. You can send these using the related link: Email: Modernised guidance team.</p>	<p>In this section</p> <p>Changes to this guidance</p> <p>Information owner</p> <p>Links to staff intranet removed</p>
--	---	---

Personal safety advice

Information owner

[About this guidance](#)

[Why personal safety advice is important](#)

[General advice on protecting and giving out information](#)

[Protecting personal information and safety - using computers](#)

[Protecting personal information and safety - exposure to identity theft](#)

This page tells you about this version of the personal safety advice guidance and who owns it.

Version	3.0
Valid from date	26 July 2013
Policy owner	Andy Boorman
Cleared by director	David Pennant
Director's role	Director – crime directorate
Clearance date	7 June 2012
This version approved for publication by:	Richard Short
Approver's role	Assistant director, modernised guidance team
Approval date	25 July 2013

Changes to this guidance can only be made by the modernised guidance team (MGT). If you think the policy content needs amending you must contact the policy team, using the related link: CI inbox, who will ask the MGT to update the guidance, if appropriate.

The MGT will accept direct feedback on broken links, missing information or the format, style and navigability of this guidance. You can send these using the related link: Email: Modernised guidance team.

In this section

[Changes to this guidance](#)

[Contact](#)

Links to staff intranet removed