10 golden rules for staff handling personal data

All staff handling personal data should remember:

- data security is your personal responsibility; know the rules for handling the data in your care and stick to those rules rigidly
- before making data available to anyone else, make certain you have the authority, including the legal power, to release it
- misuse of data or breach of security procedures could be considered to be misconduct warranting a disciplinary investigation

10 golden rules

1. Never access personal or protectively marked information, unless it is part of your job and you have a business need to do so.

2. Never give out personal or protectively marked information either over the phone or in any other way, unless you are absolutely sure who you are giving it to and that they are entitled to that data.

3. Observe a clear desk policy. Never leave personal or protectively marked information out on your desk when you are not around and always 'lock' your computer before leaving your desk.

4. Choose your password carefully and never reveal it to anyone else.

5. Challenge anybody you see in your building who is not wearing an appropriate security pass.

6. Never take personal or protectively marked information out of the office without permission and always handle it according to the rules. Never use removable media (such as a memory stick, CD-ROM or laptop) unless it is business-critical that you do so and it is encrypted to a Home Office-

Related links

HR and learning

› Security of official information

External links

› Email: HO security unit – asset protection enquiries
› Email: UKBA information management team

approved standard.

7.
Keep your laptop, BlackBerry, phone and any official papers secure at all times. Never leave them unattended.

8.
When working outside the office environment, you must ensure that any conversations or telephone calls are not overheard and that information cannot be seen by others.

9.
Always make sure that you know what protective marking the information should have and stick to the rules for that level of protection.

10.
When emailing personal or protectively marked information beyond the secure government network, send only what you absolutely need to and ensure that it is encrypted to a Home Office-approved standard.

For further help or guidance on personal data security matters, speak to your manager. Alternatively, if you work in HQ, email 'HO security unit – asset protection enquiries' and if in the UK Border Agency, the UKBA information management team.

For more guidance relating to information security, follow the related link to the 'Security of official information' section.

Page Tools

› Add to my favourites