

Press Release

For immediate release

Date: 18 June 2010

Confidential personal information stolen from Kent Police

Kent Police is taking remedial action after the Information Commissioner's Office (ICO) found it in breach of the Data Protection Act (DPA). An investigation concluded that Kent Police policies and procedures regarding the transportation and storage of personal information away from the office were limited in scope and required further clarification.

The action follows the theft of documents containing confidential personal information. The documents were stolen from the boot of a police officer's car while parked overnight at a residential address. The information was passed to a local police station after being found the following day in a nearby street by a member of the public.

Enquiries revealed that the officer had not used his secure briefcase to transport the papers, nor had he been provided with a secure storage facility at his home.

Adrian Leppard, temporary Chief Constable of Kent Police, has now signed a [formal Undertaking](#) to ensure that staff whose roles require them to have access to confidential information outside the office are provided with secure transportation and storage facilities. The policies covering the transportation, storage and use of personal and protectively marked

information will also be clarified, and all staff will be made aware of their requirements.

Sally-anne Poole, Enforcement Group Manager at the ICO, said: "It is essential that police forces ensure the correct safeguards are in place when storing and transferring personal information, especially when it concerns highly confidential information. A lack of awareness of data protection requirements can lead to personal information falling into the wrong hands."

A full copy of the Undertaking can be viewed here:

http://www.ico.gov.uk/upload/documents/library/data_protection/notices/kent_police_undertaking.pdf

Please see below for our good practice note on how organisations should treat the security of personal information:

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security%20v%201.0_plain_english_website_version1.pdf

ENDS

If you need more information, please contact the ICO press office on 020 7025 7580 or visit the website at: www.ico.gov.uk

Notes to Editors

1. The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:
 - The policies covering the transportation, storage and use of personal data and protectively marked information are clarified and all staff are made aware of their requirements;

- Staff whose roles require them to have access to personal data and/or protectively marked information outside the office are provided with secure transportation and storage facilities;
 - The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.
2. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
 3. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003
 4. Organisations can now sign the Personal Information Promise to demonstrate their commitment to protecting people's personal information by visiting the website at www.ico.gov.uk
 5. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk. Alternatively, you can find us on Twitter at www.twitter.com/ICOnews
 6. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
 - Fairly and lawfully processed
 - Processed for limited purposes
 - Adequate, relevant and not excessive
 - Accurate and up to date
 - Not kept for longer than is necessary
 - Processed in line with your rights
 - Secure
 - Not transferred to other countries without adequate protection