

**Press release**

**For immediate release**

**28 May 2010**

## **1000 data breaches reported to the ICO**

With the number of breaches involving people's personal information reported to the Information Commissioner's Office (ICO) [reaching 1000](#), the privacy watchdog is urging organisations to minimise the risk of mistakes. Staff need simple procedures on how to handle personal information with appropriate training to ensure the importance of personal information is fully understood.

Many data security breaches are a result of human or technical error. Mistakes include staff disclosing personal details to the wrong people and automated machines which send letters out to the wrong addresses. The ICO maintains it is essential that the protection of people's personal information is part of organisations' culture and DNA.

David Smith, Deputy Commissioner, said: "We all know that mistakes can happen but, the fact is that human error is behind a high proportion of security breaches that have been reported to us. Extra vigilance is required so that people's personal information does not end up in the wrong hands. Organisations should have clear security and disclosure procedures that staff can understand, properly implement these and ensure that they are being followed by staff. Staff must be adequately trained not just in the value of personal information, but in how to protect

it. The ICO's [Guide to Data Protection](#) and our tips for avoiding wrongful disclosure will help minimise the risks of security breaches occurring. We are keen to work with organisations to prevent breaches happening in the first place and to help ensure that things are put right when they do go wrong."

*Top tips – protecting personal information from wrongful disclosure*

- Are you sure that you know who you are disclosing personal information to? Have you checked that they are genuine and that they are entitled to the personal details that they are asking for?
- Beware of the dangers of email. Be very careful when selecting recipients of personal information from drop down lists to get the right ones. Do not click on 'reply to all' and automatically include all the copy recipients in your disclosure of personal information. For more sensitive information simple email disclosure may not be sufficiently secure
- Check that automated systems e.g. for stuffing envelopes are working properly and do some dip sampling to verify this
- Beware of window envelopes. Make sure that only the name and address can be seen through the window
- Check the positioning of screens particularly in open areas or by windows where they might be seen by members of the public
- Train your staff in the risks of wrong disclosure and make sure that they don't get careless about who they are passing information on to

The ICO has produced a plain English [Guide to Data Protection](#) to provide businesses and organisations with practical advice about the Data Protection Act. The guide is intended to help organisations safeguard people's personal details and comply with the law. The guide takes a straight-forward look at the principles of the Data Protection Act and uses practical, business-based examples.

## **ENDS**

A copy of the breach table is available here:

[http://www.ico.gov.uk/upload/documents/library/corporate/research\\_and\\_reports/breach\\_notification\\_spreadsheet\\_may2010.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet_may2010.pdf)

If you would like more information, please contact the ICO press office on 020 7025 7580 or visit the website at: [www.ico.gov.uk](http://www.ico.gov.uk)

### **Notes to Editors**

New powers, designed to deter data breaches, came into force on 6 April 2010. The Information Commissioner's Office (ICO) can now order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act. The power to impose a monetary penalty is designed to deal with the most serious personal data breaches and is part of the ICO's overall regulatory toolkit which includes the power to serve an enforcement notice and the power to prosecute those involved in the unlawful trade in confidential personal data.

1. Whitehall departments and many NHS organisations are obliged to inform the ICO when a data breach occurs.
2. The guidance on monetary penalties can be downloaded from the ICO website at [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specia\\_list\\_guides/ico\\_guidance\\_monetary\\_penalties.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specia_list_guides/ico_guidance_monetary_penalties.pdf)
3. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
4. 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
5. For more information about the Information Commissioner's Office subscribe to our e-newsletter at [www.ico.gov.uk](http://www.ico.gov.uk). Alternatively, you can find us on Twitter at [www.twitter.com/ICOnews](http://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

7. Examples of common personal data losses include:

- Loss of paper documents – documents containing mental health records relating to 1970 patients were reported missing in December 2009. It appeared they were lost during transit with an external courier
- Loss of unencrypted memory sticks – a memory stick containing social services information concerning 40 children was found in a public street in Stoke-on-Trent
- Loss of unencrypted CDs – a CD containing personal data relating to 9140 pension fund members was mislaid by South Yorkshire Pensions Authority