



Information Commissioner's Office

Press Release

For immediate release

18 December 2009

Shropshire Council found in breach of the Data Protection Act

The Information Commissioner's Office (ICO) has found Shropshire Council in breach of the Data Protection Act following the loss of an unencrypted memory stick containing sensitive information relating to a large number of adult social care clients and members of staff.

The memory stick, which contained a social care management database including sensitive health information, was lost during a postal transfer from the council's office to a contractor in Cardiff. The ICO has established that the memory stick also contained records that were excessive for their purpose and out of date.

Shropshire Council has worked closely with the ICO to ensure that lessons are learned. The Council has signed a [formal Undertaking](#) to ensure that databases only contain relevant and up to date information and that information is only transferred to portable devices where absolutely necessary. The Undertaking also requires the encryption of portable and mobile devices used to store and transmit personal data and for staff to be made fully aware of the Council's policy for storage of personal data.

Mick Gorrill, Assistant Information Commissioner, said: "It is essential that organisations ensure the correct safeguards are in place when storing and transferring personal information, especially when it relates to such sensitive issues. Information must be kept safe, secure and up to date – these are important

principles of the Data Protection Act. I am pleased that the council has taken action to guard against security breaches of this nature.”

A copy of the Undertaking can be downloaded here:

http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx.

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 Third and Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:
 - (1) Databases should only contain information relevant for their purpose and for the process of transfer;
 - (2) Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted by no later than 30 April 2010 using encryption software which meets the current standard or equivalent;
 - (3) Personal data should only be transferred to removable media when absolutely necessary. Where possible, sensitive personal data should be accessed remotely or hand-delivered. All other post should be adequately tracked and protected;
 - (4) Adequate checks are carried out on contractors' staff to ensure that data processors are complying with the data controller's policy in respect of the storage and transfer of such data ;
 - (5) The policy covering the transfer, storage and use of personal data is reviewed to ensure compliance with the Act, particularly in respect of the security of the means of transfer and relevance of the data transferred;
 - (6) Staff are aware of the data controller's policy for the storage, use and transfer of personal data and are appropriately trained how to follow that policy;
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 is an independent body with 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. 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

5. 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