

Press Release

For immediate release

02 June 2010

West Berkshire Council takes action after losing children's personal data

West Berkshire Council is taking remedial action after the Information Commissioner's Office (ICO) found it in breach of the Data Protection Act (DPA) following the loss of a USB stick containing the sensitive personal information of children and young people.

The memory stick, which was unencrypted and not password protected, contained, among other things, information relating to the ethnicity and physical or mental health of the children. The ICO found that unencrypted devices, in operation before the council introduced encrypted memory sticks in 2006, were still being used by members of staff. Further enquiries revealed staff had not received appropriate training in data protection issues and monitoring of compliance with the council's policies was found to be inadequate. This is the second data security incident reported by West Berkshire Council within six months.

Nick Carter, Chief Executive of West Berkshire Council, has now signed [a formal Undertaking](#) to ensure that portable and mobile devices used to store and transmit personal data are encrypted. Staff will also be made fully aware of the council's policy for the storage of personal data and receive appropriate training on data protection and IT security issues.

Sally-anne Poole, Enforcement Group Manager at the ICO, said: "It is essential that organisations ensure the correct safeguards are in place when storing and transferring personal information, especially when it concerns sensitive information relating to children. A lack of awareness and training in data protection requirements can lead to personal information falling into the wrong hands. I am aware that staff have been provided with encrypted USB sticks since 2006 but older devices were not recalled. I am pleased that the council has now taken action to prevent against further data breaches."

A full copy of the Undertaking can be viewed here:

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

Please see below for our guidance page on encryption:

http://www.ico.gov.uk/news/current_topics/our_approach_to_encryption.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 Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:
 - 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 using encryption software which meets the current standard or equivalent;
 - Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;
 - Compliance with the data controller's policies on data protection and IT security issues is appropriately and regularly monitored;

- 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