



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Press Release

23 July 2009

Neath Port Talbot County Borough Council breaches Data Protection Act

Following a breach of the Data Protection Act, Neath Port Talbot County Borough Council is taking remedial action, including the encryption of portable and mobile devices - such as laptops and other portable media - which are used to store and transmit personal data.

A memory stick containing information relating to 65 children was lost by a council employee and was not password protected or equipped with encryption software.

Ken Sawyers, Chief Executive of Neath Port Talbot County Borough Council, has signed an Undertaking to assure the Information Commissioner's Office that personal information will be kept secure in future. The council will also make staff aware of its policy regarding the storage of personal information and ensure they are appropriately trained on how to follow that policy.

Mick Gorrill, Assistant Information Commissioner, said: "I urge all organisations to restrict the amount of personal information that is taken off secure sites. I am pleased the council reacted responsibly by reporting the breach to the ICO and took remedial action. The council is implementing a number of changes to protect personal information in the future and I hope other organisations follow suit."

Failure to meet the terms of an Undertaking is likely to lead to enforcement action by the ICO. A copy of the Undertakings can be downloaded from

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 Undertaking notes that Neath Port Talbot County Borough Council will ensure:
 - 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 on how to follow that policy;
 - The policy covering the storage and use of personal data is followed by staff;
 - The data controller shall implement such other security measures it deems appropriate to ensure that personal data is protected against unauthorised and unlawful process, accidental loss, destruction, and/or damage.
2. The Information Commissioner's Office promotes public access to official information and protects personal information. The ICO is the UK's independent influential and practical authority on information rights and responsibilities, making a difference to people
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
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