

Press Release

For immediate issue

Date: 08 July 2010

Over 9,000 child details put at risk by councils

The Information Commissioner's Office (ICO) has taken action against the London Borough of Barnet, West Sussex County Council and Buckinghamshire County Council for breaching the Data Protection Act. A systemic lack of staff training on how to handle personal information has led to the loss of sensitive personal information relating to thousands of children.

Sally-anne Poole, Enforcement Group Manager at the ICO, said: "These three councils have shown a poor regard for the importance of protecting children's personal information. It is essential that councils ensure the correct preventative 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."

A theft from the home of an employee of the [London Borough of Barnet](#) was reported by the council. An unencrypted, non-password protected USB stick and CDs containing the sensitive personal information of over 9,000 children and members of their families were taken. An employee had downloaded the data onto the unencrypted devices without any authorisation to do so, although it was later revealed that there was no

training provided or security in place to prevent such downloads. The ICO had conducted an audit of the London Borough of Barnet prior to this incident that had also highlighted this lack of staff training.

[West Sussex County Council](#) had a laptop stolen, also from the home of an employee, which contained sensitive personal data relating to an unknown number of children and families involved in childcare proceedings. The laptop was unencrypted and enquiries by the ICO revealed that the employee had not received any formal data protection/IT security training. It was also discovered that over 2,300 unencrypted laptops were likely to be still in use across the council's various services, although steps are now being taken to encrypt these.

[Buckinghamshire County Council](#) provided a report regarding the loss, at Heathrow Airport, of documents containing sensitive personal data relating to two children. The documents were in a plastic wallet belonging to a council social work employee who was travelling to another UK city in connection with the children's social care case. After further analysis by the ICO, it was apparent that no real thought had been given to the security of this personal data during travel. It was also revealed that some of the council's policies needed revision and that staff training in data protection was insufficient.

The ICO has found all three councils in breach of the DPA. The London Borough of Barnet, West Sussex County Council and Buckinghamshire County Council have signed formal [Undertakings](#) to ensure staff will be made fully aware of the policies of their council for the storage and use of personal data. The London Borough of Barnet and West Sussex County Council will also provide appropriate training on data protection and IT security and ensure portable and mobile devices used to store and transmit personal data are encrypted. A further audit by the ICO will be

carried out on the London Borough of Barnet within the current financial year to monitor the previous recommendations made to it.

Sally-anne Poole added: "I am particularly concerned where a public authority has previously been warned about the lack of staff training in data security. Breaches involving such large numbers of children and family members could easily have been avoided. I am pleased that all of the councils have now taken or proposed action to prevent against further data breaches."

A full copy of each Undertaking can be viewed here:

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

A copy of the ICO's latest data breach table is available here:

http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet_may2010.pdf

Please see below for our Guide to Data Protection:

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.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

London Borough of Barnet

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;
- All staff with access to personal data are made aware of the data controller's policies for the storage and use of personal data and are appropriately trained how to follow those policies;
- Compliance with the data controller's policies on data protection and IT security issues is appropriately and regularly monitored;
- The data controller shall agree to a further audit by the Commissioner within the current financial year, which will follow up previous recommendations and may cover the requirements of this Undertaking also;
- 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.

West Sussex County Council

2. 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:
 - All 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;
 - All staff are made aware of the data controller's policy for the storage, transportation 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.

Buckinghamshire County Council

3. 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:
 - Procedures are implemented to ensure that a proper risk assessment is carried out prior to the removal from the office environment of documents containing sensitive personal data, and appropriate security measures are adopted to protect such data in transit;

- All staff are made aware of the data controller's policies for the transportation, storage and use of personal data and are appropriately trained how to follow these policies;
 - Compliance with the data controller's policies on data protection 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.
4. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
 5. 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
 6. 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
 7. 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
 8. 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