www.pdpjournal.com

ISSN 1473-3498

Privacy & Data Protection

Volume 8, Issue 4

March 2008

Headlines:

- Children's qualifications online throughout adult life, p.19
- Government could face £7.5billion compensation bill, p.19
- Solicitor pleads guilty to data protection offence, p.20
- Sharper aerial pictures spark privacy fears, p.20

Inside this issue:

New CCTV code of practice published by ICO

A new CCTV code of practice has been launched in the UK by the Information Commissioner's Office.

The code replaces the earlier one issued by the ICO in 2000 (reprinted in 2001) and takes account of technical, operational and legal changes that have taken place since the original code was drawn up.

The new code states that no organisation should monitor or store private conversations, banning employers from listening in to private conversations between members of staff.

As well as advising organisations on how to use CCTV responsibly, the new code sets out what users need to do to ensure people's rights are protected.

The ICO has warned companies that fitting microphones to CCTV cameras to record people's conversations is a "highly intrusive" development, and according to the watchdog will only ever be justifiable in "highly exceptional circumstances."

Jonathan Bamford, Assistant Commissioner at the ICO, said "It is essential that organisations and businesses use CCTV responsibly in order to maintain public trust and confidence in the use of CCTV and to prevent its use becoming increasingly viewed as part of the surveillance society."

The Code of Practice coincides with new research by the ICO which reveals that 7 out of 10 people in Scotland oppose the idea of CCTV cameras which record their conversations. In addition, 56% of Scots are aware that the Data Protection Act gives them rights relating to CCTV—a massive 20% higher than the awareness demonstrated by those surveyed in London and the South East.

Ken Macdonald, Assistant Commissioner for Scotland at the ICO, said that in order to obtain public trust organisations must

(Continued on page 19)

Ban on taking electronic devices outside the workplace

The UK Cabinet Secretary, Sir Gus O'Donnell, has imposed a ban on government employees taking electronic devices outside Whitehall premises unless encrypted. The ban covers all electronic devices, including mobile phones with data storage capacity.

The clampdown is the result of the loss of a laptop by a Navy officer containing unencrypted personal data. Police said the laptop, which had held the personal details of 600,000 people and was taken from a vehicle, contained personal information which included passport numbers, National Insurance numbers and bank account details.

Such a ban has understandably had substantial effect on officials, but the Cabinet Office said government departments were prioritising the encryption process, so the most heavily used machines were brought back into use first.

The only PDA device that is deemed to be secure enough is RIM's certified BlackBerry Enterprise Server version. However, not all government BlackBerrys meet this standard. The Cabinet Office said, "It is up to the

(Continued on page 17)