



Information Commissioner's Office

Press Release

For immediate release

01 February 2010

ATL agrees to improve information security after thousands of union members' personal details are stolen

The Information Commissioner's Office (ICO) has found the Association of Teachers and Lecturers (ATL) in breach of the Data Protection Act after a laptop and memory stick were reported lost or stolen, containing the personal details of over 6,000 union members.

The laptop was the property of the ATL and contained the personal details of 6,282 union members; it was not encrypted but was password protected. The memory stick, which was not password protected or encrypted, belonged to a staff member and contained 3,366 of the same records on the laptop. Both devices, which included some sensitive personal data, were either lost or stolen from the roadside as an ATL member was packing his car.

ATL General Secretary, Mary Bousted, has now signed an [Undertaking](#) to ensure that by 28 February 2010 all portable and mobile devices used to store and transmit personal details are encrypted. The Undertaking also requires a review of the policy covering the transfer and storage of personal data. Staff will need to be made aware of this policy and prohibited from storing personal information on their own memory sticks.

Sally Anne-Poole, Head of Enforcement at the ICO, said: "I encourage organisations to prevent staff from downloading large amounts of personal data. It is vital that portable devices, including laptops and memory sticks are encrypted if they are used to store personal information. Staff members should not be allowed to keep people's

personal details, especially sensitive personal information, on their own memory sticks. I am pleased that the ATL is taking remedial steps to prevent a similar situation occurring again.”

A full copy of the Undertaking can be viewed 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 is 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 by no later than 28 February 2010 using encryption software which meets the current standard or equivalent;
- 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;
- 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;
- Staff will be prohibited from storing data on personal memory sticks;
- The data controller shall implement such other security measures as 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 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