GUIDANCE NOTE

FIRST FINES FOR DATA PROTECTION BREACHES

March 2011

The Information Commissioner has sent a strong message to businesses by imposing the first monetary penalties on two organisations for serious breaches of the Data Protection Act 1998. The fines were imposed despite both organisations voluntarily notifying the Commissioner of the breaches.

- A **£100,000** fine was imposed on Hertfordshire County Council for two serious incidents where employees in the childcare litigation unit faxed highly sensitive personal information to the wrong recipients. The first misdirected fax was meant for a barrister's chambers but was sent instead to a member of the public. The Commissioner decided that the council had taken insufficient steps to reduce the likelihood of another breach occurring.

- A **£60,000** fine was imposed on an employment services company for the loss of an unencrypted laptop containing personal information on 24,000 people who used community legal advice centres in Hull and Leicester. The laptop was issued to an employee to enable them to work from home. It was stolen shortly afterward and an unsuccessful attempt was made to access the information stored on the laptop.

When could the Information Commissioner impose a monetary penalty notice on my business?

- The Commissioner has the power to fine your business up to **£500,000** if it has committed a serious contravention of the principles set out in the legislation that is likely to cause substantial damage or distress.

- The Commissioner must be satisfied that the contravention was deliberate or your business knew, or ought to have known, that there was a risk that a contravention would occur which was likely to cause substantial damage or distress but failed to take reasonable steps to prevent it.

What steps can my business take to manage this risk?

- Ensure your business can provide evidence it recognised the risks of handling personal data and has taken action to address the issue (for example, by conducting a risk assessment).
- Implement and enforce appropriate policies, practices and procedures to avoid potential data protection breaches within your business (for example, encrypting data on laptops, flash drives and CD-ROMs).
- Pay particular attention to data protection issues where personal data of large numbers of individuals or sensitive data is concerned.
- Implement any guidance or codes of practice published by the Commissioner or other regulatory bodies that may be relevant to potential data protection breaches within your business.
- Do not allow any known issues to remain unresolved (for example, rectify any problems with your IT systems as soon as possible).

The comments in this guidance note are of a general nature only. Full advice should be sought on any specific problems or issues

ASHTON BOND GIGG
March 2011