OBEP
T. 07887 423429
olivia.whitcroft@obep.co.uk
www.obep.co.uk

TOP TIPS FOR DATA LEAVING THE OFFICE
Merton Chamber of Commerce Factsheet, October 2012

In the world of data breaches, we frequently see something going wrong when data leaves the office. Mistakes such as mis-addressed emails or letters, or laptops and files stolen from home, have resulted in regulatory investigations and fines of up to £325,000. This factsheet sets out some top tips which organisations and staff can take to minimise the risks of data and devices falling into the wrong hands.

SENDING INFORMATION TO SOMEONE ELSE

What the organisation can do:

- Identify circumstances in which data should or shouldn’t be sent to someone else.
- Establish appropriate methods of transfer for different types of information taking into the risks and impact of unintended disclosure (e.g. encrypted media or emails).
- Maintain controls and checks over any third parties used to transfer information.
- Determine steps to be taken if something goes wrong.
- Communicate to staff the appropriate procedures and risks.

What each member of staff can do:

- Read and follow the organisation’s policies and procedures.
- Consider the risks of misuse once the communication is sent. Will the information be outside of an organisation’s security controls (e.g. personal email accounts)?
- Double-check names, numbers and addresses prior to sending.
- Ask the recipient to acknowledge receipt (and follow up if they don’t).
- Report if something goes wrong – don’t try to hide it.

TAKING INFORMATION OUT OF THE OFFICE

What the organisation can do:

- Identify when it is appropriate or inappropriate to take data and devices out of the office.
- Provide secure means of transporting data (e.g. encrypted devices, lockable cases).
- Carry out risk assessments of external premises. Consider additional facilities for home working.
- Determine steps to be taken if something goes wrong.
- Communicate to staff the appropriate procedures and risks.

What each member of staff can do:

- Read and follow the organisation’s policies and procedures.
- Only take documents and devices out of the office if there is a legitimate business or organisational need, and don’t take more information than you need.
- Don’t take sensitive documents or devices to places where there is a high risk they may go missing (e.g. the pub!).
- Take sensible steps to protect data and devices at home, as you would in the office.
- Report if something goes wrong – don’t try to hide it.

Olivia Whitcroft, solicitor and principal of OBEP (www.obep.co.uk), October 2012

This factsheet provides general guidance on data protection issues and should not be relied upon as legal advice.