Appendix 1

Data Handling Guidelines

updated 19th December 2008

This document summarises the information you need to know in order to ensure that you handle the council's data and information safely and securely.

In 2007 CLT approved eight principles that reflect the council's vision for how we collect, store, use and share our information and knowledge. These principles are:

- We share information appropriately and lawfully
- Our information is open and accessible
- We use information ethically
- Our information is accurate and fit for purpose
- We all have responsibilities for our information
- We regard information as a Leeds City Council resource
- We value information as an asset to the Council
- We have the skills and confidence to act according to these principles

It is increasingly important that people are aware of their responsibilities and the purpose of this message is to raise awareness and provide guidance as to what we all should be doing.

- This advice is **not** about stopping people undertaking their role.
- This advice **is** about people being risk-aware in terms of the data and information they handle.

Things you need to know:

Data Protection Act principles – we all need to adhere to the following DPA principles to make sure that people's 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 their rights
- Secure
- Not transferred to other countries without adequate protection

Mobile devices (such as council laptops, PDAs and memory sticks that support flexible working) **create additional potential risks for data security.**

The difference between password protection and encryption. We often assume that password protection is sufficient to secure our data, but this is not necessarily the case. In many instances password protecting a file may make us feel more secure about the data within it. In reality, this offers very little additional protection. Encryption of data offers much more protection, but can be expensive or time consuming. The key thing to think about is "How important is the data I am trying to protect?" If you are working with data which:

- Is sensitive, commercial or restricted
- Could cause or encourage physical or financial harm to a person or company (including identity theft)
- Identifies someone individually

Then you must take extra care to ensure that the data you are working with is safe. For example, storing this data on a memory stick without adequate protection could leave the Council liable under the Data Protection Act if the stick were to fall into the wrong hands.

Definitions

- **Personal data.** This is data relating to identifiable living individuals.
- **Sensitive data.** Under the DPA this is personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, mental / physical health, trade union membership, sexual life and commission or alleged commission of any offence
- **Commercial data.** This is data provided to or by the Council which contains commercial details, such as pricing structures or contract terms, which should only be available to a restricted audience, for example, those involved with a tender or purchase. If this data is released to third parties such as competitors it may give them an unfair advantage in current or future negotiations.
- **Confidential data.** This is information which has explicit conditions attached to its subsequent use or disclosure, or where the conditions are obvious or implied e.g client/lawyer, client/social worker, and which is not readily available by other means.
- **Restricted data.** This is a particular type of data defined by central government. It has a number of defining characteristics, but the important thing is that this definition is applied by someone else, for example the Police or the Home Office. If you are dealing with restricted level information, you will be told this is the case, and must take extra care.

Home working

- If you are working from home and using any of the data types described above you should use an LCC laptop, and should not be using your own personal PC to process or store this kind of data. You should not use a memory stick to store or transport any of these types of data.
- Ensure any data you are working with at home is accurate and up to date.
- Any work-related documents you do use on your home computer should be deleted when you have finished working with them.

The risks of poor data security

There are numerous risks to poor data security and you'll be familiar with most of these:

- Risk to the customer
- Risk to the organisation in terms of reputation
- Loss of trust of the public, partners, staff and audit bodies;
- Increased external scrutiny
- Impact on operations if customers or partners stop providing data
- Financial loss
- Court cases

What you can do today

- Any personal data that needs to be taken off-site should be encrypted. ICT Services will soon be introducing a disk encryption solution to all Council laptops. You should not take personal data off site using any other method than a Council laptop
- Report any losses of laptops or memory sticks to your manager and the ICT Help Desk
- Always delete files from laptops and memory sticks when you have finished with them
- Familiarise yourself with the Data Protection Act principles.
- If you don't **have to** move data around – don't do it!
- Apply an appropriate level of caution to handling data and information.
- If you are carrying data on a memory stick, only take with you the data you need.

What is happening to improve information security?

There are a number of things planned to help improve information security, these include:

- Encryption of laptop hard drives
- Encryption of PDAs
- Improved secure remote access for employees with LCC laptops
- Further awareness raising on a range of information management and data quality related issues.

Questions and queries

If you have any questions or queries, please contact:

Zoe Cooke in Legal Services (24 74238) or your local representative for Data Protection Issues

ICT Service Desk (24 76565): Loss of mobile devices, data security issues.

Information and Knowledge Management Team (39 52264): Information Governance Issues