Bolton Council

Report to:	Corporate Issues Scrutiny Committee		
Date:	4th February 2008		
Report of:	Director of Legal and Democratic Services	**Report No:**	14
Contact Officer:	Carl Wiper, Corporate Information Manager	**Tele No:**	331031
Report Title:	**Security of Council data**		
Confidential / Non Confidential: *(delete as approp)*	(***Non-Confidential***) This report does **not** contain information which warrants its consideration in the absence of the press or members of the public		
Purpose:	To provide an overview of the security of the Council's main data sets and measures being taken to protect them.		
Recommendations:	The Committee is asked to consider the security of our information systems and work underway to safeguard them.		
Decision:			
Background Doc(s):	The attached report provides summary answers to questions posed to Officers by the Chair of the Committee in relation to our datasets and details the work being undertaken to promote information security in the Council		

Background Information

1. Introduction

The Committee has asked the Council to address the following questions regarding data that we hold:

1) A broad outline of the data
2) What systems are in place to ensure that this data is protected from access both internally & externally?
3) Who is able to access the data i.e. level of employee?
4) Can this data be burned onto any disc, and does this operation require specific authorisation, and at what level?
5) Do we transport data out of the confines of the Town Hall?
    a) is this electronic or manual?
    b) if manual who are the companies we use, and what audits do we carryout on these companies and how often, and are any risk assessments carried out as regards these processes?
6) Who do we send data to?

In the light of recent data losses in the public sector, it is timely that we should review our security arrangements, and indeed work on information security was already underway in the Council in 2007. To date, as far as we are aware, we have suffered no significant data losses, but this is no cause for complacency, and we are continuing to address this issue.

2. Broad outline of the data

The Council currently holds over two and a half thousand different sets of records, in electronic or paper form, relating to all aspects of its work. Just over half of these contain either personal data or information which is sensitive or confidential for other reasons. Many of these are small, local collections but some are major business systems.

In the context of this report it is not possible to provide answers to all of the questions for all of our data sets, but we have used this structure to give an overview of current arrangements. For the purposes of the report we have gathered information in respect of the following main data sets:

Department	Data set	Coverage
Adults	Contracts	Service users receiving home care and service providers
Adults & Environmental Services	FLARE	Information on businesses and inspections
Adults	Epi-info	Information on disease status and GPs
Adults	Direct Payments	Recipients of direct payments
Adults	Supporting people	Service providers and service users
Adults	Adult disability provider services	Disability carers
Bolton at Home		

	OHMS (Open Housing Management System)	Tenants and Homes for You applicants
Chief Executives	CASS/OPAS & paper records	Occupational health data
Chief Executives	ORACLE (HR)	Personnel records
Adults/ Children's	CAREFIRST	Social care client records
Children's	EMS	Client files, exclusion files, pupil data
Children's	CORE	Connexions - Assessment forms, client information, special needs
Corporate Resources	ORACLE (payroll)	Payroll data
Corporate Resources	Academy and Anite (document image processing – DIP system)	Council Tax, Housing & Council Tax Benefit
Corporate Resources	Data accessed by Customer Services	Oracle CRM system, CCCG (Complaints system), Email Centre, Witness (call recording), WOSS (Web One Stop Shop), PARIS (payments system), OHMS, access to other corporate systems listed elsewhere.
Corporate Resources	ORACLE(Income Section)	Accounts receivable, mortgages, car loans
Development and Regeneration	Data held by Regeneration and Economic Development	Information on employment and skills clients
Legal and Democratic Services	STRAND (electoral registration)	Electoral Register
Legal and Democratic Services	Mountain (Coroners)	Doctors' reports, personal details, inquest verdicts

3. Systems in place to protect data

Databases and electronic data sets are protected by the Council's network security arrangements, i.e. the network is protected by the Council's firewall and staff require a password to access the system. Network users are prompted to change their password at regular intervals and are advised not to share passwords and to keep them secure. Where data is held on shared drives ("G drives"), these are only accessed by the team concerned and other users would have to request access.

The electronic databases listed above additionally require their own passwords (with the exception of the DIP system) and specific controls are in place. Precautions are taken for particularly sensitive data sets e.g. for Carefirst, non-social care staff require special authorisation to access the system and in Occupational Health and Safety users sign a confidentiality agreement.

4. Access to the data

For all the data sets we looked at, it was reported that access is restricted to staff in the relevant team, with certain exceptions noted below. In most cases, though not all, the password gives role based access, i.e. users are able to view and amend only certain fields, depending on their role. Staff in the Customer Services Division are able to access a wide range of databases in order to do their work, once they have received training e.g. Academy, Anite DIP, OHMS, Carefirst, Oracle, Smart Card, Complaints database, Email centre, Web One Stop Shop, PARIS (payments system). CSD are currently reinforcing the message to staff that they should only access these systems for specific and authorised use.

In the case of Carefirst, the departmental information systems support team have access for help desk purposes and the supplier (OLM) also have access to enable support

The OHMS system is also accessed by Housing and Council Tax Benefit staff and partner housing associations that require it in order to do their job.

In Occupational Health and Safety there is a system of role-based access to paper files also i.e. users can only see parts of the files depending on their role. OHS also take precautions to ensure data cannot be accidentally seen by visitors at the front desk.

5. Copying the data

In the case of the smaller databases, data could be copied ('burned') on to a CD; for the major databases the data itself cannot be copied directly, but reports can be run on the database and then exported to a format such as Excel, in which it could be burned to disk; in addition it is technically possible to take screen shots and copy them onto disk. However in practice there are control measures because only authorised users have passwords to access the system. It should be borne in mind also that although not all sections have CD/DVD writers, where data can be copied it could be copied to a memory stick rather than burned to a CD. We have issued specific guidance on memory sticks as noted under *Current work on information security* below.

6. Transporting the data & Transferring data to other organisations

The drive towards partnership working means that data often needs to be shared with other organisations as well as with bodies such as the Audit Commission for checking purposes.

As part of the National Fraud Initiative, the Audit Commission requires us to send copies of certain datasets every two years. Last time this included payroll, market stall rents, housing rents, creditors, private care home residents and insurance claimants. The Audit Commission have recently also asked for council tax and electoral register data. The data has so far been sent in the way requested by the Audit Commission, namely on CD, in unencrypted form, by registered post. However, the Audit Commission are setting up a secure electronic transfer system for use in future.

We are also required to send Housing Benefit and Council Tax Benefit data to DWP monthly. This has previously been sent on disk by courier (TNT or Parcel Force) and is receipted and signed for but DWP have suspended this until a secure electronic system is in place.

Other examples of data transfer are:

- Payroll send data electronically and encrypted via BACs to transfer money to people's bank accounts. They also send encrypted data to the Inland Revenue via Electronic Data Interchange (EDI) for year end returns. Pensions data is sent electronically to Tameside and is password-protected. Some data is sent by post to Trade Unions but Payroll have asked to send this via email. Payroll also receive printed payslips from MBA via their courier service
- In OHS data is burned to disk and sent to the database suppliers Warwick International for upgrades. It is sent by Fujitsu, and a confidentiality agreement is in place with them.
- Connexions send data electronically to DCSF via secure upload.
- Accounts receivable send invoices and reminders electronically to MBA printers via Fujitsu
- The electoral register is sent by email to various government bodies and to credit reference agencies which are entitled to receive it.

In general we have not carried out audits of intermediary companies, but we send data by the means requested by government bodies such as the Audit Commission and in some case we have confidentiality agreements as noted above. To date we have not had any reports of such data going missing.

We are mindful of the recent statement by the Information Commissioner that if unencrypted data sent on disk goes missing and damage or distress is caused to individuals, he will regard this as a *prima facie* breach of the Data Protection Act. Where we need to share data with other agencies we intend to use secure electronic transmission wherever possible and to encrypt data if it is absolutely necessary to send on disk by courier.

In addition to these regular data transfers, there are occasions when it is necessary to send data, for example on social care clients, by email to another agency. We are aware that this is not inherently secure and we are looking at ways to address this, for example by encryption or secure data transfer.

In addition, the move towards mobile and home working means that data may be taken out of the secure environment of the Council's network. CICT are looking into encrypting hard disks on laptops and they have the capability to wipe a Smart phone remotely if it is lost. Memory sticks can also pose a particular risk. Furthermore, it is sometimes necessary to take paper files with client data out of the office. We have recently issued guidance on the use of memory sticks and we are producing guidance on security in mobile working as part of our information security work.

7. Current work on information security

At the beginning of 2007 the Council recognised that more work needed to be done on information security. This is being taken forward by the Corporate Information Unit in co-operation with CICT, Internal Audit and the Risk Manager. The Council now has an Information Security policy, which was adopted before the well-publicised national security breaches occurred. We have also produced briefings and guidance notes for staff, all of which are available on our intranet. Planned work for this year includes a security incident reporting system, with which all staff can report actual or potential breaches, a toolkit for assessing information security risks and procedures for disposing of confidential records. This will be supported with more communications to staff on security matters. It is envisaged that the Corporate Information Unit will oversee this, while CICT continue to deal with IT security matters, Information Officers advise departments on security, and Internal Audit check the efficacy of information security measures we have in place.

8. Conclusions

In order to do its work the Council holds a vast amount of personal and confidential data in a large number of databases and filing systems. Statutory obligations, partnership working and support arrangements may require this data to be shared with external organisations. Developments in technology can allow us to increase levels of security but they can also create new risks, as can changes in working patterns.

To date the Council is not aware of any significant data loss. Nevertheless, there is no room for complacency and the Council takes the issue of information security very seriously. In addition to network and system security measures already in place, the Council is working on encryption and secure transfer of data and is issuing guidance to staff on specific security issues as well as identifying responsibilities for information security matters.

9. Recommendations

The Committee is asked to consider the security of our information systems and work underway to safeguard them.