Part I
Release to Press

Meeting: **AUDIT COMMITTEE**

Agenda Item:
7

Date: **16 January 2008**

SECURE EXCHANGE OF CONFIDENTIAL ELECTRONIC DATA

Author - Henry Lewis	Ext No. 2496
Lead Officer - Henry Lewis	Ext No. 2496
Contact Officer - Henry Lewis	Ext No. 2496

1 PURPOSE

1.1 To outline the key systems in place within the Council to safeguard the exchange of personal data to third parties. To advise the Committee of proposals to improve upon existing procedures and to address the Council's responsibilities for safeguarding both physical and electronic data generally.

2 RECOMMENDATIONS

2.1 That the Committee notes that a central register setting out details of personal electronic data exchanged with third parties will be implemented as a priority by the end of January 2008.

2.2 That the Committee notes that a review of training and guidance provided to staff on the subject of the Data Protection Act will be undertaken by the end of February 2008.

2.3 That the Committee notes that an officer led Security Panel will be set up to establish the overall level of compliance with ISO 17799, the international code of practice covering information security management and will report with recommendations by September 2008.

2.4 That the Committee notes that a decision on whether to participate in the Government's Secure Information Network will be made by the end of April 2008.

3 BACKGROUND

3.1 This report has been written in the context of HMRC's widely publicised loss of millions of electronic personal records which included customers' bank details. The report is intended to provide assurance to the Council that a similar situation will not arise here.

The Council has a duty to comply with the Data Protection Act 1998 when considering whether to exchange personal information with third parties and to consider the seven principles laid out in the Act when considering an appropriate means of doing so.

3.2 The Council holds personal information relating to residents and/or our staff on many IT systems, particularly name and address information. Bank details are held on comparatively few systems:

- the Northgate Housing System
- the Pericles Housing Benefits and Council Tax system
- the Antares Payroll and Human Resources system
- the Integra Financial system (which holds suppliers' bank details)

3.3 There are two principal types of organisation with which the Council routinely exchanges personal information held on our ICT systems:

- public sector agencies
- ICT system suppliers

3.4 Public Sector Agencies

We exchange information with the following agencies for the following reasons.

We provide monthly information to the DWP and HMRC about benefit claimants for the purposes of fraud prevention. Information included all personal information relating to the claims, which often includes bank details, details of other family members and declared income.

We provide an annual return to HMRC detailing payments to landlords and interest payments to businesses as well as an annual Council Tax return.

There is also a 2 yearly return to the Benefit Fraud Inspectorate including details of benefits claimants, housing tenants, creditors and Council Tax payees. This may include bank details for some claimants.

We provide details of staff salaries, their dates of birth, names and addresses to the Inland Revenue on an annual basis.

Finally we provide similar details to Serco, who process pensions on our behalf.

3.5 ICT System Suppliers

Most of our ICT System Suppliers have access to the systems that they support and the data contained within them. This is necessary to allow them to investigate problems arising with the systems, to implement patches and to perform other routine application support tasks. However:

- suppliers are limited in being able to access only those systems that they support
- the number of staff accessing systems from any supplier is tightly restricted

- supplier access is password controlled. They also have to arrange for access to the system with the Council in advance and explain why they need access to the system/s

Further than that, the Council relies upon the suppliers' published security policies, which will normally cover the way they vet their staff and their systems for ensuring compliance with their policies. Suppliers' security policies are assessed as part of the evaluation process when procuring new systems.

The Council may also have to send copies of databases to system suppliers where the database is required by the supplier to diagnose system problems. For example, the Council has had to sent a copy of the Pericles database to the system supplier this year and the database included details of all benefit claimants' bank details and bank details for residents paying Council Tax by direct debit.

3.6 **Methods of Data Transmission**

The method of transmission depends upon the facilities available at the receiving organisation. It may be via secure File Transfer Protocol, which in practice means that data is secure and encrypted and sent electronically. Alternatively, it may be sent via courier or in the post using a traceable method of delivery, such as Royal Mail's special delivery service. In that case data will have been written to a CD or DVD, the file secured with a password (notified separately to the receiving authority by e-mail). A strong password is always used, involving at least 8 characters and a mixture of alphanumeric characters and upper and lower case characters.

3.7 The bulk transfer of electronic data which includes personal information is always undertaken by either an experienced member of staff in the Council's E-Government & Business Systems SDU, by the Payroll Manager or occasionally by a member of the Council's Housing Benefit Investigation Team. By restricting the opportunity for staff to exchange information in this way, the Council is able to exercise stronger control.

This does not preclude any member of staff with access to personal information e-mailing it to a third party, albeit this could not happen in large volumes. Staff working in areas where sensitive personal information is involved will have had training in the Data Protection Act and guidance should be available to them. A priority proposal arising from this brief review is to ensure that training has been sufficiently comprehensive and that guidance is up to date and effectively communicated.

4 REASONS FOR RECOMMENDED COURSE OF ACTIONS AND OTHER OPTIONS

4.1 Based upon the analysis undertaken, the Council is only exchanging information with third parties when required to do so by statute or in compliance with the Data Protection Act. The arrangements in place governing the transmission of data are robust and we are taking reasonable steps to ensure that third parties, such as IT system suppliers, are taking their responsiblities seriously under the Act. It should also be noted that there have been no instances of data exchanged with third parties going missing in recent years.

Nonetheless, given the understandable sensitivity surrounding these issues some

enhancements to current processes and guidance will be implemented as a priority:

- a corporate register will be implemented to provide an at a glance record of bulk transfers of electronic personal data. The register will identify the officer responsible, details of the data transfer and will be authorised at Head of Service level
- training and guidance provided to staff about the Data Protection Act will be reviewed and improved upon where necessary

In the medium term the Council along with other Hertfordshire authorities is establishing whether participating in the Government Secure Information (GSI) Network represents value for money. This network, whichallows completely secure transfer of electronic information amongst participating authorities, is becoming increasingly relevant to the Council as requirements for information sharing amongst public sector bodies increase.

4.2 This review has focused upon the exchange of personal electronic data with third parties. There are of course many other scenarios which could result in personal data being lost. These include inadequate controls over physical data, unauthorised access to ICT systems, ICT systems being subjected to electronic attack and fraudulent behaviour on the part of staff. All these issues are dealt with in ISO 17799, the code of practice for Information Security Management. Although the general view is that the Council is well protected against most threats, a piece of work will be undertaken in the medium term to assess the Council's compliance with the standard. Initially, this will take place by convening an Officer led security Panel, comprising key Heads of Service and/or their representatives from Legal Services, Human Resources, Payroll, Revenues and Benefits, Finance and Facilities Management , chaired by the Head of E-Government & Business Systems.

5 IMPLICATIONS

5.1 Legal Implications

Based upon the analysis undertaken, the arrangements in place governing the exchange of electronic personal data to third parties are sufficient to meet the Council's responsibilities under the Data Protection Act 1998.

BACKGROUND

None

APPENDICES

None