REPORT TO THE Final Accounts and Audit Committee	Report No. 7
Date of Meeting	**7 April 2008**
Title of Report	**Data security**
Link to Corporate Priorities	
Public Report	Yes

Summary of Report

To present to the committee a review of the security of personal data sent outside of the council.

Officer Recommendations

That the report, risk assessment and associated actions/control measures be endorsed.

Other than those implications agreed with the relevant Officers and referred to below, there are no other implications associated with this report.

Financial Implications	Legal Implications	Community & Environmental Implications	Human Resources Implications	Equality & Diversity Implications
None	None	None	None	None

Contact Officer	Pete Barnett Head of ICT 01249 706280 pbarnett@northwilts.gov.uk

1. Introduction

1.1 Following a number of high profile occurrences of the loss of personal data by Central Government departments, a review of personal data sent outside of North Wiltshire DC has been carried out.

2. Options and Options Appraisal

2.1 Option 1: That the report, risk assessment and associated action plan is endorsed by the committee.

2.2 Option 2: That the committee suggests other actions that could be taken.

3. Background Information

3.1 As part of its day to day business the council is required to send a range of data outside of North Wiltshire DC. An audit and review of personal data sent outside of the council has recently been carried out which focussed on services who send customer and/or employee data to other public sector organisations or outside companies as part of their business. For the purpose of the review, data was defined as that which contained names, addresses and one other identifier (e.g. national insurance number, bank account number, date of birth etc).

3.2 The review concentrated on services who send personal data in bulk to other organisations/companies as that is the most likely area where the loss of such data could have potentially serious impact on the council and its customers and employees.

3.3 The council has an Information Management and Data Security (IM&DS) policy (a copy will be provided on request) which was approved by the Personnel Licensing and Administration Committee on 8th May 2006 (minute P114). The committee delegated authority to the Information Management Group to make minor amendments with major changes going back to PLA for approval.

3.4 The policy is very comprehensive and provides guidance on a large number of areas (detailed in Section 1 - Executive Summary) covering the security of both printed and electronic information. In general terms the policy covers the areas of most concern following the central government data loss. Breaches of the policy are dealt with under the council's disciplinary process. Monitoring of the policy is also in place, particularly with regard to email usage and internet access, although this is more difficult to enforce with printed material.

Of particular interest will include:-

Section 4.4	Deliver and Collection of Goods
Section 5.6	Security of Media in Transit
Section 7	Use of Electronic Equipment
Section 9	Email Usage Policy

3.5 There is a separate policy which deals with the disposal of PC's, this is currently being updated to include disposal of media (USB sticks, CD's DVD's etc) as well as remote devices such as PDA's. The intention is for this to be added as a new section within the overall IM&DS Policy. PC's are currently disposed of to European WEEE standards and data destroyed to the Infosec 5 data security standard (the standard recommended by CESG, the UK National Technical Authority for Information Assurance.

3.6 All staff are required to read the policy and sign to confirm this, existing staff were provided with awareness sessions when the new policy was launched. Awareness of the policy and its contents is provided for all new starters as part of the induction process.

3.7 A separate policy for members was approved by the Personnel Licensing and Administration Committee on 5th March 2007 which includes references to the IM&DS policy.

4. Risk Analysis

4.1 A risk assessment with related control measures which will feed into the action plan is included at appendix 1. This will be monitored on a regular basis by the Information Management and Data Security Group.

4.2 Control measures are already being put in place to mitigate risks identified in the risk assessment. Any loss of personal data is likely to have a high impact on the council and its customers and staff, however the control measures implemented have reduced the likelihood of a loss of personal data to low.

Appendices:	• **Audit of sensitive data risk assessment**
Background Documents Used in the Preparation of this Report:	• **Information Management and Data Security Policy**

Previous Decisions Connected with this Report

Report	Committee & Date	Minute Reference
Information Management and Data Security Policy	Personnel, Licensing and Administration	P114