Part I – Release to Press

Meeting: **Audit Committee** **Agenda Item:** **8**

Portfolio Area: Resources

Date: **7 March 2011**

DATA PROTECTION ACT COMPLIANCE

Author – Paul Froggatt Ext 2212 & Henry Lewis Ext 2496

Lead Officer – Scott Crudgington Ext 2185

Contact Officer – Paul Froggatt Ext 2212 & Henry Lewis Ext 2496

1. PURPOSE

1.1. To update Members on the Council's current arrangements for fulfilling its responsibilities under the Data Protection Act.

2. RECOMMENDATIONS

2.1. That the report be noted.

3. BACKGROUND

3.1. The current Data Protection Act has been in force since 1998. The regulation and enforcement of the Act has been largely passed to the Information Commissioner who also has the principal role of enforcing the related Freedom of Information Act and Environmental Information Regulations.

3.2. It has only been, however, in the last year that the Information Commissioner had the power to serve mandatory penalties for certain breaches of the Data Protection Act. It is clear that the Information Commissioner tends to make full use of these powers and also clear that he takes very seriously the loss of personal data by data controllers whether or not the loss has been accidental.

3.3. In November Hertfordshire Council was fined £100,000 after confidential and sensitive personal data was faxed inadvertently to a member of the public on two occasions. Although the breach was reported to the Information Commissioner a substantial fine was imposed as the Commissioner was satisfied that the contravention was likely to cause substantial damage or substantial distress.

3.4. There have subsequently been other cases involving other local authorities including fines against Ealing and Hounslow Councils in February for the accidental loss of personal data on laptops which were not encrypted. It should perhaps be noted that in these cases adequate procedures were in place but simply not followed.

3.5. The underlying legal requirement covering the loss of data is contained in the Seventh Data Protection Principle which provides that "Appropriate technical and

organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." The Act further provides that "Having regard to the state of technological development and the cost of implementing any measure, the measures must ensure a level of security appropriate to:

A. The harm that might result from such unlawful or unauthorised or unlawful processing or accidental loss, destruction or damage that are mentioned in the seventh principal

B. The nature of the data to be protected."

3.6 In the light of the case referred to above referring to Hertfordshire County Council the Leader of the Council requested a report to this Committee on the measures taken by Stevenage to ensure that such data losses do not occur.

4. REASONS FOR RECOMMENDED COURSE OF ACTION AND OTHER OPTIONS

4.1. The Council addresses data protection in two ways. Firstly, in house training and advice on all aspects of the Data Protection Act is provided for the Council and Stevenage Homes Limited. This training also covers the closely related Freedom of Information Act and Environmental Information Relations and more distant Human Rights Act. Secondly, and bearing in mind that all of the data loses involved digital media, there are the technological and procedural aspects of security.

Compliance and Awareness Training

4.2. The general responsibilities relating to training and advice are undertaken by the Legal Section, where one of the officers is designated as the Information Officer. He deals with the various requirements on the Council imposed by the Data Protection Act including the Council's biennial registration. The greater part of this role, however, is dealing with information requests including, in the case of the Data Protection Act, data subject access requests by individuals who have the right to be supplied with information which the Council holds on them. In performing these functions the Information Officer is supported by the Borough Solicitor.

4.3. The programme of internal training in place since 2009 arranged by the Training and Development Manager is mandatory for all new entrants to the Council. This includes a course presented by the Borough Solicitor and ICT Systems, Security & Standards Officer which covers a general introduction to data protection and analysis of the data protection principals including the Seventh Data Protection principles set out above. The training also covers IT security issues and focuses upon how systems should be used to minimise the risk of data loss occurring.

4.4. The Training and Development Manager is currently arranging a general awareness programme for all officers (not just new entrants) of the Council and to incorporate mandatory procedures for data security in the staff handbook.

4.5. The Council has a number of policies which relate to the Data Protection Act, personal use of IT and issues of data security. These are all available on the Council's Intranet.

Technological Aspects to Security

4.6. There are two main types of risk to data security that the Council is required to mitigate. Firstly, the Council is required to put in place sufficient controls to prevent third parties gaining unauthorised access to data. Secondly, the Council is required to take reasonable measures to prevent data loss perpetrated by staff or others authorised to access the information.

4.7. The Council has made great progress relating to the safeguarding of its network in recent years, thus preventing unauthorised access to information from third parties. The Council has successfully met the exacting requirements of the Code of Connection document which dictates the security standards required to access the Government Connect Secure Extranet (GCS(X)). The Council has also received favourable results from the annual health check which independently assesses the Council's network security.

4.8. Following the security incident in April 2010 which resulted in two day's downtime across the Council's network, security risks were assessed by the ICT Team in a lessons learned report that was reported to the Audit Committee. This resulted in the implementation of a number of short term measures to reduce the risk of a further virus being spread and to reduce the risk of data loss. In particular:

- The use of portable media devices, such as memory sticks has been significantly reduced
- All laptops are now fully password protected
- All staff are encouraged if working from home to use the Citrix connection. This means that data is not stored on their home computers or on the hard disks of their lap tops, but is held centrally, securely on the Council's servers in Daneshill House
- Staff who work from home and access sensitive personal data, such as Benefits Assessors, are provided with additional security tools to protect the data and to prevent data loss

4.9 Notwithstanding the above, there is still further work to be completed to fully mitigate the risks of data loss, notably to encrypt all laptops and to introduce encrypted memory sticks. A project to undertake this work is underway and is being overseen by the Council's Information Security Group. A copy of the initiation document for this work is attached at Appendix A to this report. The work will be completed by June 2011.

5. IMPLICATIONS

5.1. Financial Implications

5.1.1 There are no financial implications. All work referred to in the above report has been fully resourced.

5.2. Legal Implications

5.2.1. The legal issues relating to data protection are set out in the main body of this report.

6. BACKGROUND DOCUMENTS

- There are no background documents.

7. APPENDICES

- ICT Security Improvement – Project Definition Document