AUDIT COMMITTEE	AGENDA ITEM No. 4
7 June 2012	PUBLIC REPORT

Cabinet Member responsible:	Councillor Seaton, Cabinet Member for Resources	
Contact Officer:	Diane Baker, Head of Governance	Tel. 452259

DATA INCIDENT RESPONSE POLICY

RECOMMENDATIONS
FROM : Helen Edwards, Solicitor to the Council
1. To approve the Data Incident Response Policy.

1. ORIGIN OF REPORT

1.1 This report is submitted to the Committee following a referral from the Monitoring Officer.

2. PURPOSE AND REASON FOR REPORT

2.1 The purpose of this report is to seek the Committee's approval for a Data Incident Response Policy.

2.2 This report is for the Committee to consider under its Terms of Reference No. 2.17: To consider the Council's arrangements for corporate governance and agreeing necessary actions to ensure compliance with best practice.

3. TIMESCALE

Is this a Major Policy Item/Statutory Plan?	**NO**

4. DATA INCIDENT RESPONSE POLICY

4.1 All data controllers, including the Council as a whole and all 57 councillors individually, have a responsibility under the Data Protection Act (DPA) 1998 to ensure appropriate and proportionate security of the personal data which they hold. Anyone who processes personal information must comply with the eight principles of the DPA, which make sure that 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 your rights
- Secure
- Not transferred to other countries without adequate protection

4.2 This policy puts into place a formal procedure for dealing with any breaches of the DPA which may occur and focuses on the steps to be taken once a breach has been identified. A copy of the draft policy is attached at Appendix 1.

4.3 The loss of personal information can have serious financial, legal and reputational implications for public authorities. The Information Commissioner, who upholds information rights in the public interest, promotes openness by public bodies and regulates data privacy for individuals, has the power to serve a monetary penalty notice on a data controller for loss of personal information. For example two councils have recently received fines of £80,000 and £70,000 following the theft of laptops, which were stolen from employees' homes, and which contained the personal details of individuals.

4.4 It is clear that if there was to be a breach of security around personal data, the Information Commissioner's Office (ICO) would expect the breach to be dealt with effectively. Introducing a policy on dealing with information security breaches serves to formalise measures we already have in place to comply with the seventh data protection principle – ensuring personal data is secure.

4.5 Whilst there is no legal obligation in the DPA for data controllers to report breaches of security which result in the loss, release or corruption of personal data, the Information Commissioner believes that serious breaches should be brought to the attention of his Office. This policy offers guidance on what those serious breaches could be and how the Council will deal with an incident.

5. ANTICIPATED OUTCOMES

5.1 That the Council will have in place a policy which will assist in meeting its responsibilities under the Data Protection Act 1998.

6. REASONS FOR RECOMMENDATIONS

6.1 A Data Incident Response Policy is considered best practice and whether we have a formal policy in place is something that would be considered by the Information Commissioner's Office if there was a serious breach in security.

7. IMPLICATIONS

7.1 The implications of this policy are that the Council will become more aware when handling people's personal information and will continue to consider the risks and consequences of losing this type of information. It was also ensure that any data breach will be properly handled and in accordance with the law.

8. BACKGROUND DOCUMENTS

Used to prepare this report, in accordance with the Local Government (Access to Information) Act 1985)

Guidance on Data Security Breach Management – Information Commissioner's Office (July 2011)

9. APPENDICES

- Appendix 1 – Data Incident Response Policy