AGENDA ITEM: 10

AUDIT & GOVERNANCE:
29 January 2013

Report of: Borough Solicitor

Relevant Managing Director: Managing Director (People and Places)

Contact for further information: Terry Broderick – Borough Solicitor (Extn.5001)

SUBJECT: INFORMATION GOVERNANCE/DATA PROTECTION

Wards affected: Borough wide.

1.0 PURPOSE OF REPORT

1.1 To enhance information governance/data protection arrangements by clarifying/ formalising governance arrangements in line with recommended good practice.

2.0 RECOMMENDATIONS

2.1 That the delegation to the Borough Solicitor at Constitution 4.2 A, B (i) para16 be amended to read: "To co-ordinate compliance with the requirements of the data protection legislation, determine requests for disclosure of personal data and act as the Council's Senior Information Risk Owner (SIRO)".

2.2 That the updated Data Protection Policy attached as Appendix 2 be approved and it be noted that a proposal for additional resources of £30,000 will be submitted to Council in February 2013.

3.0 BACKGROUND

3.1 The Information Commissioner and the Department for Communities and Local Government promote the importance of good information governance. They draw attention to the significant change that came into force in April 2010, which enabled the Information Commissioner's Office (ICO) to order organisations to pay up to £500,000 as a penalty for serious breaches of data protection principles. Recent penalties include a £130,000 penalty imposed on Powys County Council and £250,000 for the Scottish Borders Council. There have been 19 local authorities "fined" for breaches of security to date.

3.2 The ICO and DCLG recommend some actions that all local authorities can and should take to reduce the likelihood of falling foul of data protection requirements. These include recommendations to:

- Have identified and trained a board-level individual to act as the Senior Information Risk Owner (SIRO);
- Continuously make staff aware of the existing information governance policies and guidelines, emphasising the importance of following them in practice and that a breach of policy will be regarded as a disciplinary matter;
- Ensure all staff undertake regular and relevant information governance training.

It is to be noted that the coverage of "information" extends beyond personal data.

3.3 Currently, the Council's Data Protection Policy places day to day responsibility for compliance with the Act, including data security, with the Managing Directors and Heads of Service within their respective areas of authority under delegated arrangements. Within each Service, a Data Protection Link Officer(s) has/have been appointed by Heads of Service to undertake administration of data protection and to assist in compliance. That role includes ensuring all systems are appropriately notified to the ICO, awareness of the Data Protection Act 1998 (DPA), control of processing of data in compliance with the Councils requirements and assisting in responses to subject access requests.

3.4 These in Service arrangements are aided by the central resource providing general data protection advice. These are coordinated by the Borough Solicitor (part of an overarching role). The central resource includes the Senior Admin & Electoral Services Officer (DP Officer), whose responsibilities include maintenance of the notification of processing with the ICO and the internal register of subject access requests, development of corporate procedures and the first point of contact for subject access requests. Training resources are to be provided from the corporate resource provided through Human Resources (or within a Service, where particular needs are identified). Legal officers provide assistance for the strategic aspects and more complex matters as part of my coordinating role. Formerly the Head of ICT provided the role of developing and enforcing the ICT & data Security Policy, although the change in arrangements through engagement of OCL requires some changes to this allocation of responsibility.

3.5 The policy recognises also that all officers and members have a duty to observe the principles of the DPA when handling personal data.

4.0 ISSUES

4.1 The Council holds a vast amount of data about customers and employees, and its services and properties. This is held both electronically and in paper form. It is vital that proper arrangements are in place to appropriately safeguard this information. The importance of proper information security has been borne out by the number of data losses which continue to be reported across the public sector, showing that threats to our information security are ever-present.

4.2 It is essential to have technical measures in place to mitigate risk, such as encryption of devices (e.g. a programme of encryption of laptops is currently being rolled out); to have policies and procedures to dictate how data/information should

be used and to carry out training and awareness-raising to remind staff to meet requirements. There is also another important element in the information security framework, namely governance. In this context this means that we must have clear responsibilities and reporting lines to ensure that information security is managed properly and that we have a comprehensive view of the state of information security across the Council.

4.3 A Local Government Association (LGA) / Government Connect (GC) document *'Business Case for Creating a SIRO Role'* (Appendix 1) acknowledges that often there is someone already undertaking many of the functions of a SIRO, it recommends that information security is given a higher profile with clear governance arrangements in place to ensure that information security is managed properly. It advises that the key roles in the governance of information security are the SIRO, the Information Security Group (ISG) and the Information Asset Owners (IAOs). All staff, members and partner organisations also have a responsibility to follow security policies.

4.4. <u>SIRO</u>

LGA guidance and best practice recommends that the SIRO:

- Is the officer who is ultimately accountable for the assurance of information security at the Council
- Champions information security at Directorate Service Head (DSH) level
- Owns the corporate information security policy
- Provides an annual statement of the security of information assets for the Annual Governance Statement (as part of the audit process)
- Receives strategic information risk management training at least once a year

The SIRO is not intended to be a new post but rather a newly defined set of responsibilities for an existing 'board-level' post. It is not concerned solely with ICT, but takes a broader view of our information assets as a whole, in any form. I already undertake a coordinating role and it is therefore proposed that my post should be so designated.

Feedback from other local authorities indicates that the SIRO resides within a Corporate Governance or Legal area of responsibility.

4.5 <u>Information Governance/Data Protection Working Group (the Group)</u>

The LGA guidance recommends that a working group should be set up by the Chief Officer Steering Group or Executive Management Team to look into the state of information security in the Council. This group should be composed of representatives from Legal and Democracy Services, Finance, ICT, Internal Audit, Risk Management and the Data Protection Officer. Representatives of other sections should attend meetings as required. The Group should develop policy and guidance on information security and maintain a reporting procedure for information security breaches. The Group would support the SIRO and its remit would be to:

- Review and develop the Council's information security strategy.
- Review and develop information security policies and guidance and ratify changes to these, including ongoing review of relevant Council Policies, e.g.

Data Protection Policy and ICT and Data Security Policy and Retention and Disposal Policy.
- Coordinate a data protection review within Services, to include: compliance, cataloguing of data resources, training requirements, document assessment, e.g. for privacy notice/customer notification.
- Assist in a coordinated approach to Service Specific Data Protection Procedures
- Assist with management of security risks in projects through the project life cycle
- Review all reported security breaches and report them regularly (and immediately where appropriate) to the SIRO and onward to Government Connect where appropriate
- As appropriate, report information security breaches to the Information Commissioner via the SIRO
- Promote awareness of information security by all officers and Members
- Plan, develop and deliver training on information security in consultation with the Transformation Manager.

It is proposed that the current Data Protection Working Group be renamed the Information Security/Data Protection Working Group with the above terms of reference so as to more closely accord with the LGA guidance. Service Heads and their respective Link Officers would continue to service this group which the SIRO would chair.

4.6 Information Asset Owners (IAO)

LGA guidance and best practice recommends the formal nomination of IAOs. IAOs should be senior managers/software system supervisors across the Council who are currently responsible for the main information systems and information assets.

Relevant senior managers/software personnel have been identified by Heads of Service for formal nomination as IAOs and the role is recognised in the updated Data Protection Policy, attached at appendix 2. In terms of information security their responsibilities would be:

- To manage security, compliance and risks associated with their information assets
- To carry out an annual assessment of information risk as part of risk management
- To ensure that staff accessing the systems are made aware of security issues and acceptable use and receive training as necessary
- To ensure that information security incidents are reported via the Council's information security incident reporting procedure
- To ensure that actions are taken to remedy breaches
- To classify information assets in line with corporate policies. Using a classification scheme for sensitive and confidential information.
- To receive information risk management training annually
- To consider on an annual basis how better use could be made of their information assets within the law

5.0 FINANCIAL AND RESOURCE IMPLICATIONS

5.1 In order to deliver and embed the revised arrangements a one-off £30,000 additional support be sourced to assist Heads of Service in implementing the updated policy and arrangements. This would be used to procure a temporary post enabling the relevant processes etc to be put in place. A bid for the resource would be put forward for consideration at February Council.

6.0 SUSTAINABILITY IMPLICATIONS/COMMUNITY STRATEGY

6.1 Robust information systems have a role in delivering against all of the themes of the community strategy.

7.0 RISK ASSESSMENT

7.1 Good information governance arrangements will establish clear accountability and reporting lines across the Council in relation to data protection and information security. They will assist the Council in securing compliance. The recent internal audit of data management has highlighted certain areas of service delivery which require attention. The consequences of security or other information handling incidents can be significant, particularly relating to personal data loss, in both financial and reputational terms.

Background Documents

There are no background documents (as defined in Section 100D(5) of the Local Government Act 1972) to this Report.

Equality Impact Assessment

The decision does not have any direct impact on members of the public, employees, elected members and/or stakeholders. Therefore no Equality Impact Assessment is required.

Appendices

Appendix 1: The LGA/GC document *'Business Case for Creating a SIRO*
Appendix 2: Updated Data Protection Policy
Appendix 3: Current Data Protection Policy