



Committee and Date

Audit Committee

19 September 2012

2 pm

Item

5

Public

INFORMATION RISK POLICY

Responsible Officer Ceri Pilawski

e-mail: ceri.pilawski@shropshire.go.uk

Tel: 01743 252027

1. Summary

The Cabinet agreed at its meeting on the 6th June 2012, to the approval of a new policy covering the Council's governance of the information it uses for service delivery, the Information Risk Policy, see **Appendix A**. This policy sets out a framework for the Council to manage its information to relevant standards to support effective service delivery and meet its compliance obligations, not only for the protection of information, but also in making information proactively available to meet transparency and openness requirements. It supports the Council's Data Protection, Information Security and Records Management Policies in accordance with Local Government Association Data Handling Guidelines for Local Government.

Within this framework there are responsibilities outlined for Audit Committee, Internal Audit and external assessors and this report brings those responsibilities to the attention of members.

2. Recommendations

Members are asked to consider and endorse with appropriate comment their responsibilities under the Information Risk Policy.

REPORT

3. Risk Assessment and Opportunities Appraisal

- 3.1 The establishment of an effective framework to govern the Council's information and within that, clarity as to everyone's roles and responsibilities will enable it to use information with confidence in supporting service delivery, meet its

compliance obligations and minimise the risk of loss, inappropriate access or disclosure of information.

3.2 Should the Council's information not be handled to appropriate standards there is potential risk for:

- inability to provide necessary services to our customers;
- breach of legislation;
- loss, inappropriate access to or disclosure of information;
- hindrance to or loss of information assets or facilities;
- reputational damage;
- financial penalties.

3.3 The recommendations contained in this report are compatible with the provisions of the Human Rights Act 1998. There are no direct environmental, equalities, consultation or climate change consequences of this proposal.

4. Financial Implications

4.1 There are no direct financial implications as a result of introducing the policy.

4.2 If measures are not in place to mitigate risks to an appropriate level there is the possibility of financial penalties.

5. Background

5.1 Good governance of information is vital for the Council to operate effectively. The information we hold is an asset. If we use it well it provides many opportunities as it helps to make our business more efficient and improves the services we offer to the public.

5.2 As the Council looks for new ways to deliver services it is imperative that information can be used and shared legitimately with confidence, not only by the Council, but also by our service partners. The Council needs a clear view of what information it holds, how it is used and that it is managed appropriately to deliver services efficiently.

5.3 The Council faces a constantly changing environment in how the information it processes is required to be used. Over the past year we have seen new requirements to publish datasets for senior salaries, payment data and contract information. New legislation, such as the Protection of Freedoms Act 2012 (enacted 1 May 2012) brings other new requirements, such as extending the Freedom of Information Act to include publishing datasets and the type of companies caught by the Act, in addition to modifying how information used within a range of Council services can be used. Clear ownership of information assets, with a knowledge of the how the information can be used is key at a service level. Information Asset Owners will be required to understand the legislative requirements that affect the information within their remit and be accountable for its compliance.

5.4 As and when areas of responsibility change, it is vital that information assets are considered and managed to maintain business continuity and ownership re-assigned.

Robust processes are required to ensure:

- the quality of data, enabling business decisions to be made and information published and shared in confidence
- information is being used legitimately
- a level of security commensurate to the value of information is in place
- information is shared responsibly
- ownership and management of information is clear
- business records are maintained where required

5.5 The attached policy sets out the roles and responsibilities required of individuals and groups to provide a culture that properly values, protects and uses information for the public good. Audit Committee's role within this is to ensure that information risks are assessed and mitigated to an acceptable level. This assurance can be provided from the role of Internal Audit and external assessors who review and report against compliance of the policy and standards around information governance.

List of Background Papers (This MUST be completed for all reports, but does not include items containing exempt or confidential information)

Cabinet report and minutes, 6th June 2012 Information Risk Policy

Cabinet Member (Portfolio Holder) Keith Barrow (Leader of the Council) and Brian Williams (Chairman of Audit Committee)

Local Member n/a

Appendices

Appendix A The Information Risk Policy