Report to Cabinet

Subject: Information Security Policy

Date: 4 April 2013

Author: Corporate Director and Council Solicitor & Monitoring Officer

---

Wards Affected

Not applicable.

Purpose

To seek approval for the Information Security Policy.

Key Decision

This is not a Key Decision

Background

1.1 The Council currently has an over-arching IT Policy which has been in place for some time. The existing Policy is a framework within which IT facilities are provided across the Council. It covers a range of topics including how access is granted to the network, acceptable use of the facilities and good practice when setting passwords etc. For a variety of reasons, including the requirement to achieve and maintain external IT security related compliance and to ensure that all users of the Council's IT facilities are aware their data handing responsibilities, a new Information Security Policy is being proposed.

1.2 The Data Security Group [DSG], which consists of the Council Solicitor & Monitoring Officer, Service Manager – Customer Services & IT and the Service Manager – Audit & Risk Management, has been working on producing new Information Security Policies for some time. Initially a number of draft policies were procured externally and the DSG agreed to go through them to tailor them to the Council's specific circumstances. Unfortunately progress was slow, predominantly due to resource issues.

1.3 In May 2012, the DSG reviewed its position on policy development. It was agreed that instead of having a raft of policies covering individual aspects of information security, one comprehensive Information

Security Policy, would be created. This work has now been done and a comprehensive Information Security Policy (which appears at Appendix 1) produced and approved by the DSG. The Policy has also been subject to internal consultation with Service Managers.

1.4 The Policy sets out the legal framework for information security along with clearly defined responsibilities. It also includes arrangements for the following:

- Access Controls
- Remote working
- Mobile devices
- Procurement of Systems
- Secure Disposal
- Protective Marking
- Managing security incidents

It is intended that the Policy will replace the existing IT Policy.

1.5 The DSG has also produced a Personal Data Security Commitment Statement to be signed by staff which lists in a simple document the obligations on staff set out in the Information Security Policy. This is to be a companion document to the Policy. A copy of the Statement appears at Appendix 2 for information.

1.6 Information resources are vital to enable the Council to conduct its business and deliver services to residents, businesses and visitors. The Council must have appropriate arrangements in place to ensure the integrity, security and confidentiality of that information. In the absence of such protection, the Council is at risk of a breach of security which could compromise those essential information resources. This could result in the Council being unable to maintain service levels; failing to comply with legal requirements and being exposed to financial penalties and facing reputational damage. Such a breach could also have an impact on those individuals whose information is accessed or compromised. This Policy is designed to provide an appropriate level of protection to the information for which Gedling Borough Council is responsible.

Proposal

2.1 It is proposed that Cabinet approves the Information Security Policy which is attached as Appendix 1 to this report.

2.2 The importance of information security needs to be reinforced across the Council. A training programme is being developed to raise awareness of the Information Security Policy across the Council and ensure that staff are aware of their responsibilities and accountable for their actions. It is intended that the training is made available to all

employees. No extra resources will be needed to provide this training as it will be delivered in house.

Alternative Options

3 Not to approve the Information Security Policy, which could result in the Council being unable to maintain the highest standards of information security.

Financial Implications

4.1 Any costs associated with the introduction and implementation of the Policy will be met within existing budgets.

4.2 Failure to comply with information governance legislation could result in the Information Commissioner imposing a monetary penalty of up to £500,000.

Appendices

5 Appendix 1 – Information Security Policy.

Appendix 2 - Personal Data Security Commitment Statement.

Background Papers

6 None identified.

Recommendation(s)

THAT the Information Security Policy be approved.

Reasons for Recommendations

7 To ensure that the Council has a robust policy in place which protects the Council and the information it holds by providing a clear framework for preventing, monitoring and responding to information security breaches.