POLICY & RESOURCES COMMITTEE	Agenda Item 39 Brighton & Hove City Council

Subject:		**Information Security Policy Framework**
Date of Meeting:		**11th July 2013**
Report of:		**Executive Director Finance & Resources**
Contact Officer:	**Name:**	**Mark Watson** **Tel: 29-1585**
	Email:	**mark.watson@brighton-hove.gov.uk**
Ward(s) affected:		**All**

FOR GENERAL RELEASE

1. SUMMARY AND POLICY CONTEXT:

1.1 This briefing note seeks agreement by the committee to the implementation of an Information Security Policy framework.

1.2 Our residents, customers, visitors and partners expect that their information is held securely and confidentially, is accurate, and is available when and where it may be needed for their benefit. However, threats to the integrity and security of that information exist internally through misuse, accidental or malicious loss or disclosure, and externally from hackers and disgruntled troublemakers both within and outside the UK.

1.3 An Information Security Policy framework (and its individual policies) creates the working environment in which information can be protected in an organisation. Defining and enforcing corporate security policies ensures that the council has an efficient, consistent working environment, has the ability to defend against internal and external threats and shows due diligence to the people it serves. Effective information security increases public confidence and helps avoid any potentially damaging action being taken against the council such as litigation or large fines from the Information Commissioners Office (ICO). Fines for individual data breaches are now commonly reaching £150,000 and have a maximum of £500,000. Effective information security is also essential to ensure ongoing access to the government's Public Service Network (PSN) through its Code of Connection (CoCo). The Cabinet Office has recently introduced a zero tolerance policy meaning that any organisation which does not meet its stringent security requirements cannot share data with other public agencies. This is a business critical requirement for a very large number of our services.

2. RECOMMENDATIONS:

2.1 That the Policy & Resources Committee agrees the Information Security Policy framework attached as Appendix 1 to this report.

2.2 That the Executive Director, Finance & Resources, be granted delegated powers to approve ICT related policies, protocols and guidance subject to compliance with the Information Security Policy Framework.

3. RELEVANT BACKGROUND INFORMATION:

3.1 An Information Security Policy framework has been created and can be visualised as a pyramid. An overarching corporate information security policy setting out the organisation's approach and commitment to information security is at the top. This policy is underpinned by area specific policies which form the second layer; these cover areas such as Data Protection, information handling and remote working. The policies are based on the various standards with which the council must comply. Policies are further supported by guidance, process and procedure at the third layer.

3.2 This Information Security Policy framework will define the working practices for all staff, partners and members for all data and information that is collected, created, managed and processed by and within the council.

3.3 The council operates under various duties which require it to appropriately protect its information. The key pieces of relevant legislation are;

- Data protection Act (1998),
- Freedom of Information Act (2000),
- Computer Misuse Act (1998),
- Human Rights Act (1998).

3.4 As a data controller within the terms of the Data Protection Act, the council must also adhere to the data protection principles. These aim to protect the rights of the individual and set out how an organisation should process personal or sensitive personal information. This includes ensuring that information is only used for a lawful purpose and that *all* necessary steps should be taken to adequately protect such information.

3.5 In addition to legal compliance requirements, the council is also under a contractual obligation to comply with the requirements of the PSN Code of Connection and the Information Governance (IG) Toolkit if it is to continue to work with Central Government departments, other local authorities or Health organisations.

3.6 To place this in an operational context; the Revenues and Benefits Service relies heavily on our GCF (Government Secure Intranet Convergence Framework) connection which enables communication with the Department for Work and Pensions. Without this connection the Revenues and Benefits service would be unable to operate. Further, a key element of the GCF service is the Government secure email solution known as GCSx. Users across the council rely on this service to send sensitive information to other government departments. The GCF physically connects multiple government departments and enables wide information sharing; the risks to Government, through allowing multiple users onto its network, are therefore significant. In response to this risk the Government requires that all public services wishing to sign up to the GCF meet the requirements of the PSN Code of Connection ('CoCo'). This is broadly based on industry best practice standards such as ISO 27001. These requirements are closely linked with the requirements of the Data Protection Act. The IG Toolkit is the NHS's version of the CoCo; services such as Adult Social Care and Public

Health connect into the NHS using an N3 connection which is only available through meeting the requirements of the IG Toolkit.

3.7 The common theme running through all of these duties is the requirement for a security policy framework. The council does currently have policies in place; however, historically they were developed by individual business areas following various approval methods and are published in various locations. This has resulted in a less than coherent policy set with contradictory controls and guidance which is both confusing for staff and makes the policies unenforceable for the organisation.

3.8 In order to consolidate these disparate policies, a simplified, coherent framework has been developed that is easy to understand and apply, presented in a single repository, managed and kept up to date by the corporate centre for information.

4. COMMUNITY ENGAGEMENT AND CONSULTATION

4.1 Not applicable

5. FINANCIAL & OTHER IMPLICATIONS:

Financial Implications:

5.1 There are substantial fines of up to £500,000 that can be applied by the Information Commissioner's Office for individual data breaches. Without a clear policy framework for managing and controlling information security, the risks identified in the report are more likely to be realised and therefore consideration of additional financial risk provisions would need to be given within the council's budget setting process and Medium Term Financial Strategy. There is therefore a potential direct (fines) and indirect (risk provisions) financial consequence of not putting in place a robust framework.

5.2 The ICT Investment Plan 2013-16, approved by Policy & Resources Committee on 21 March 2013, includes up to £6m of investment to improve much of the council's ICT infrastructure and data security, including investment in improved 'Identify and Access Management' to strengthen controls over access to customer and citizen's information and accounts.

Finance Officer Consulted: Nigel Manvell Date: 10/06/13

Legal Implications:

5.3 The proposals in this report will assist the Council in complying with its legal obligations regarding data protection, freedom of information and human rights as well as additional requirements which may be imposed by regulatory authorities.

5.4 Although the power has been delegated to the Executive Director, Finance & Resources, it is expected that the Information Governance Board, which includes representatives from a cross service of Officers and the Head of Law, will normally be consulted on significant new policies to ensure that wider legal, governance and practical considerations are taken into account.

Lawyer Consulted: *Abraham Ghebre-Ghiorghis* *Date: 26//06/13*

Equalities Implications:

5.5 An Equalities Impact Assessment (EIA) will be conducted against any part of the implementation of the security programme which results in a change to user functionality. Service and or customer service impacts will be addressed by relevant services where identified.

Sustainability Implications:

5.6 None

Crime & Disorder Implications:

5.7 None

Risk and Opportunity Management Implications:

5.8 Implementation and enforcement of a security policy framework is a key component of the wider mitigation activity required to ensure that the council is compliant with it's obligations under the Data Protection Act, the PSN Code of Connection and the IG Toolkit for N3.

5.9 Failure to comply with the DP Act could result in:

- Further action being taken by the ICO. This may be a fine (up to £500,000 per breach) and/or enforcement action.
- Heightened risk of data loss which may result in financial penalties. Loss or theft may result in action being taken by the ICO.
- Inability to provide public services.
- Loss of reputation and public confidence.
- Personal liability for unlawfully obtaining information, or for managers who negligently allow employees to unlawfully obtain information. The Information Commissioner is seeking to impose custodial sentences for senior managers in cases of serious negligence.

5.10 Failure to comply with the PSN CoCo could result in:

- Unannounced audit by the Communications and Electronics Security Group (CESG) and enforcement action. This is typically a 'cut off' notice which would result in GCSx mail and GCSx applications (used by Revs and Bens) being suspended. The council would not be able to work with DWP, Health or the Police if this were to happen.

5.11 Failure to comply with the IG Toolkit could result in:

- Disconnection from access to the N3 NHS network.

Public Health Implications:

5.12 Public Health is dependent on the ability to connect to and access data on the NHS network (N3). If this were not available Public Health staff would be unable to operate the service. Connection to the N3 network is subject to compliance with standards set out in the IG Toolkit, which includes the requirement to have a full information security policy framework in place.

Corporate / Citywide Implications:

5.13 In the context of ever diminishing resources and continued austerity the council must work to develop new ways of working, including sharing service delivery and close collaboration with a variety of partners. This is articulated through the Corporate Plan as the ambition to be 'A leader of the city region'. In order to build these partnerships we must be able to share information securely. To do this safely we must treat information as a valuable shared resource, operate securely and adopt common information standards.

5.14 The implementation of the policy framework will result in improved information sharing through commonality of approach both internally and with external partners.

5.15 Ensuring that we operate to the highest standards of information governance means that other agencies can be confident that BHCC can be entrusted with their information and that information provided by BHCC is of an acceptable standard.

6. EVALUATION OF ANY ALTERNATIVE OPTION(S):

6.1 There are no viable alternative options to the adoption of an updated and refreshed policy framework for information security. The current policy set is inconsistent, inaccurate, out of date and no longer fit for purpose. Lack of a refreshed and updated policy framework could lead to the negative impacts set out in section 5 above.

7. REASONS FOR REPORT RECOMMENDATIONS

7.1 In order to meet the various compliance requirements the council must implement a comprehensive policy framework.

7.2 A comprehensive policy framework is essential to the council's ability to run its daily business.

SUPPORTING DOCUMENTATION

Appendices:

1. Over-arching Information Security Policy (with policy diagram)

Documents in Members' Rooms
None

Background Documents
None