

**DRAFT INFORMATION SECURITY POLICY**

Agenda Item 7

**Portfolio Area:**

**Report Presented by:** Lesley Day, Audit, Insurance & Risk Manager

**Background Papers:** Local Government Data Handling Guidelines received 18th November 2008; CESG Guidelines

**Corporate Implications:** Please refer to table at end of report

**Options:** N/a

**Risks:** That data theft or loss could occur if an Information Security Policy is not introduced and enforced; failure to comply with requirements of Government Connect.

**Executive Summary**

The draft Information Security Policy has been produced to take into account the guidelines and requirements as set out by the Local Government Association and Government Connect.

To support the Policy, 15 Codes of Practice have currently been produced which detail the various requirements covered by the Policy.

**Decision**

To **RECOMMEND TO CABINET** that the Information Security Policy be adopted by this Authority

**Background**

The implications of information loss or theft are very serious. Criminals with access to lost or stolen information, particularly that which is highly confidential, can use it to commit identity and other fraud. Crimes are sometimes the work of opportunistic criminals but they are also carried out by organised criminal groups that possess expert knowledge of data technology.

There have been several high profile incidents of data loss in both the public and private sectors which has raised public awareness of the possible consequences and also the need for organisations to review their data security procedures which will encourage customer trust and confidence.

In November 2008, the Local Government Association produced the long awaited Local Government Data Handling Guidelines that set out the fundamental steps that every council should take to mitigate against the ever present risk.

In addition, Central Government departments are changing the way that we need to communicate with them. The authority currently uses a variety of methods, but from June 2009 we are going to be required to use Government Connect. Government Connect is a network between local authorities and government departments, and will be used to communicate with DWP and other agencies. To connect to this network we need to fulfill a number of ICT security requirements, which the Government Connect team are calling a Code of Connection.

The Information Security Policy which is currently supported by 15 Codes of Practice still requires further work on specific areas and as a result an action plan has been produced covering the following:

- Member training through e-learning pool
- Publish an Information Charter
- Enhance internal security at Causeway House
- Introduce Privacy Impact Assessments
- Assess the requirement of a Corporate Information Governance Group
- Produce a "quick glance" staff information leaflet
- Establish approved information disposal contractors

<b>Corporate Implications</b>				
<b>Financial:</b>	None			
<b>Legal:</b>	[Outline any legal implications and indicate that advice has been sought from Legal Services]			
<b>Equalities &amp; Diversity:</b>	None			
<b>Customer Impact:</b>	Data theft or loss of customer details could occur if an Information Security Policy is not adopted and enforced; Failure to comply with requirements of Government Connect could result in reduced service standards to Housing Benefit claimants			
<b>Environment &amp; Climate Change:</b>	None			
<b>Consultation/Community Engagement:</b>	Local Committees	None	Partners	None
	Public	None	Staff	None
<b>Key Decision:</b>	No			
<b>Public/Private Report:</b>	Public			
<b>Officer Contact:</b>	Lesley Day			
<b>Designation:</b>	Audit, Insurance & Risk Manager			
<b>Ext No:</b>	2821			
<b>Email:</b>	lesley.day@braintree.gov.uk			