WIRRAL COUNCIL

CABINET - 10 DECEMBER 2008

REPORT OF THE DIRECTOR OF FINANCE

INFORMATION AND COMMUNICATION TECHNOLOGIES SECURITY POLICY

1 EXECUTIVE SUMMARY

1.1 This report informs Members of proposed amendments to the Information and Communication Technologies (ICT) Security Policy last presented to Cabinet on 1 December 2005.

1.2 Members are requested to agree the Information and Communications Technology Security Policy as amended.

2. THE ICT SECURITY POLICY

2.1 The draft ICT Security Policy has been amended following consideration by the Information Strategy Group and Internal Audit.

2.2 ICT is an integral part of Council activities and is essential in the delivery of most services and in communication with partner organisations. Because of this, policies and procedures need to be laid down and enforced in order to safeguard those services and the Council interest. These include:

- the physical assets
- access to the information stored on or available through those assets
- service continuity
- users of the systems and equipment
- compliance with legislation

2.3 An agreed ICT Security Policy is essential in the light of developments in the use of:

- the broadband communications network
- mobile working
- the linking and common use of systems
- the volume and sensitivity of data held on ICT equipment and systems
- the Corporate Change Programme
- the requirements of Government Connect, which will enable the secure exchange of data with public sector partners.

2.4 Investment in ICT physical assets such as the centrally located application servers and storage area network, distributed servers, personal computers (PCs) and the communications infrastructure is significant.

2.5 The ICT Security Policy applies to the following people:

- all employees and elected Members of the Council
- all employees and agents of other organisations who directly or indirectly support or use the Council computer systems or networks
- all temporary and agency staff directly or indirectly employed by the Council.

and to all areas of ICT, including:

- PCs and associated equipment, including personal digital assistants (PDAs) and all mobile equipment and storage devices
- all servers including Unix, Novell and Microsoft based systems
- multi-function devices, printers, faxes and other reprographics equipment
- network communications
- software.

2.6 The Security Policy should be operated in conjunction with Audit Guidelines for ICT Systems, as produced and periodically updated by Internal Audit.

2.7 Members will be aware of instances of loss of sensitive data in the public sector. This has resulted in a Government review of the handling of such data and recommendations have been made with which the Council will have to comply. This will impact on the Security Policy which will be returned to Cabinet on a more frequent basis in future.

3 GOVERNMENT CONNECT

3.1 Members should be aware of the impact of the Government Connect programme on the ICT systems and information use.

3.2 Government Connect (GC) is a pan-government programme led by the Department for Work and Pensions (DWP) to provide a trusted, secure network for all Local Authorities in England and Wales.

3.3 The network is called Government Connect Secure Extranet (GCSx) and it enables secure data sharing up to “RESTRICTED” (see 3.8) level across Government. The programme has been funded by a partnership of the DWP, the Department for Communities and Local Government (DCLG) and the Department for Children, Schools and Families (DCSF) until 31 March 2011. Local authorities will bear their internal costs.

3.4 In order to connect to the GCSx, the Council must be compliant with a set of security criteria known as the Code of Connection. The general deadline for compliance is 31 March 2009 but many Local Authorities, including Wirral, have applied for an extension of up to 6 months. IT Services are currently working towards compliance by the extension date.

3.5 The DWP has issued strict deadlines by when the Authority must be joined to the secure network. After this Wirral will not be able to access such systems as the CIS (Customer Information System) database which is vital to Housing Benefits and Council Tax. GCSx will be the only means by which local authorities can communicate with the DWP after their agreed extension date. A connection is also necessary for children's services, free school meals, ContactPoint, "In and Out of Work" and "Tell Us Once".

3.6 Once connected, Wirral employees will be able to use GCMail, a secure email service, for information up to "RESTRICTED" level to communicate with other local authorities, Police, NHS, DWP, Trading Standards, Criminal Justice and Youth Justice.

3.7 Using GCSx and GCMail will save the Government time and money e.g. the cost of couriers, thus improving customer service. Its primary benefit will be that it is more secure than current methods for communication and sharing data, such as posting CDs. Attachments up to 25MB can be sent on GCMail and already some Government departments will no longer email anyone who does not have a secure email address.

3.8 There is a Government Protective Marking Scheme (GPMS) with levels of "TOP SECRET", "SECRET", "CONFIDENTIAL", "RESTRICTED" and "PROTECT". The purpose of the GPMS is to identify the sensitivity of the information and so dictate the level of security required in the handling of that information, regardless of how it is held. Only information of levels RESTRICTED and PROTECT may be exchanged over GCSx. The appropriate level is dictated by the impact of unauthorised disclosure or loss. Definition of the relevant levels is included in Appendix 2 to the Security Policy.

3.9 The requirements of Government Connect are incorporated into the revised Policy. These requirements will continue to increase and will impact on the Policy and the use of ICT equipment and information.

4 SIGNIFICANT CHANGES TO THE POLICY

4.1 The Policy has been amended to take account of the absorption of the former Wirral IT Services (WITS) and departmental IT units into the corporate IT unit, IT Services.

4.2 At Policy paragraph 2.2 further examples of non-compliance have been added.

4.3 At paragraph 2.3, reference to the requirement for individuals with knowledge of a breach of the policy to follow the guidelines in Appendix 1, Reporting an ICT Security Incident.

4.4 The introduction of a requirement that system owners authorise the access to relevant Wirral systems or information by representatives of external bodies at Policy paragraph 4.2.

4.5 The introduction in the Policy of a reference to the GPMS at paragraph 5.1(c).

4.6 A revision of password standards has been incorporated at paragraphs 6.4(a), (c) and (e).

4.7 The addition of paragraph 7.4 relating to the secure disposal of any ICT or associated equipment in compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive.

4.8 Paragraph 8.1(c) has been added to advise of the need for every device that can run anti-virus software to have an appropriate solution installed on it, and for this to be updated and maintained regularly.

4.9 Observance of the Policy by Members and staff using mobile devices is incorporated at paragraph 8.4 and the addition of Appendix 3.

4.10 At paragraph 12.3, reference to GCSx and the interception or monitoring of communications and to the prohibition by Government Connect of auto-forwarding of e-mails to accounts in a lower classification domain.

4.11 The addition of paragraph 13.2 which outlines the responsibility for the physical security of ICT facilities lies with the appropriate Building Manager in consultation with ICT system owner.

4.12 The addition of paragraph 14, relating to the need for staff security clearance checks.

4.13 Appendices are now:

1 Reporting an ICT Security Incident
2 Information Classification: Government Protective Marking Scheme (GPMS)
3 Use of Mobile Devices
4 Use of Internet and Electronic Mail Facilities Code of Practice

5 SUMMARY

5.1 The ICT Security Policy provides a framework for Members, officers and others to work within when using ICT so that the Council assets, information, systems, services and legal obligations are protected.

6. DATA PROTECTION LEGISLATION

6.1. Any Personal Data held by the Council is subject to the Data Protection Act 1998. Personal Data is defined as any information which identifies a living individual. The medium it is held on is irrelevant and this may be computer files, manual records, photographs or CCTV footage for example. I have responsibility for Data Protection compliance and this is delegated to the Information Manager. The Information Manager is responsible for ensuring that Council activities and purposes which utilise Personal Data are notified to the regulator, the Information Commissioner. The Notification can be viewed on line on the public register pages at www.ico.gov.uk

6.2 The Data Protection Act requires disclosure of Personal Data in accordance with the Notification. Additional disclosures may be allowed with informed consent or in specific documented circumstances, such as for crime prevention. All disclosures must be in accordance with current Data Protection legislation.

6.3. The eight Data Protection Principles are:

- Personal data must be processed fairly and lawfully.
- Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes must not be kept for longer than is necessary.
- Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

7 FINANCIAL AND STAFFING IMPLICATIONS

7.1 Cabinet on 22 May 2008 agreed the one off costs of procurement and installation of a server and an additional firewall for Government Connect to be funded from the Efficiency Investment Budget at a cost of £29,000.

7.2 Ongoing charges to be met by the Council from 2011/ 12 are uncertain but based on the existing known costs could be in the region of £56,000 per annum.

7.3 With regard to staff resources required, IT Services has developed the plan for implementation within existing resources.

8. EQUAL OPPORTUNITIES IMPLICATIONS

8.1 There are no equal opportunities issues arising from this report.

9 HUMAN RIGHTS IMPLICATIONS

9.1 There are no specific Human Rights issues arising out of this report.

10 LOCAL AGENDA 21 IMPLICATIONS

10.1 There are no Local Agenda 21 issues arising from this report.

11 COMMUNITY SAFETY IMPLICATIONS

11.1 There are no direct Community Safety issues arising out of this report.

12 PLANNING IMPLICATIONS

121.1 There are no planning implications arising out of this report.

13 LOCAL MEMBER SUPPORT IMPLICATIONS

13.1 There are no specific issues arising out of this report.

13 BACKGROUND PAPERS

14.1 Government Connect Programme Code of Connection and Guidance.

14.2 International Standards Organisation (ISO) 27001 Information Security Management Systems.

15 RECOMMENDATION

15.1 That the amended Information and Communications Technology Security Policy be agreed.

IAN COLEMAN
DIRECTOR OF FINANCE

FNCE/279/08