WIRRAL COUNCIL

CABINET

2 SEPTEMBER 2010

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 23 July 2009.

1.2 Members are requested to agree the Information and Communication Technologies Security Policy as amended.

2. THE ICT SECURITY POLICY

2.1 The ICT Security Policy has been amended following consideration by the Information Strategy Group, the Information Manager 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 Change Programme

- the requirements of Government Connect, which enables 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
- all volunteers engaged directly or indirectly 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.

3 LOCAL GOVERNMENT DATA HANDLING GUIDELINES

3.1 Members will be aware of instances of loss of sensitive data in the public sector. This resulted in a Government review of the handling of such data and recommendations have been made with which the Council will have to comply. The amendments to the IT Security Policy implement the recommendations of the Local Government Data Handling Guidelines within Wirral.

3.2 Further amendments to the IT Security Policy will be required as additional recommendations are agreed.

4 INTERNAL AUDIT RECOMMENDATIONS

4.1 Internal Audit has recommended that the Policy be updated to clarify that corporate backups taken by IT Services are for use in disaster recovery purposes only (6.4 below).

5 GOVERNMENT CONNECT – REVISION OF ADMINISTRATION RIGHTS

5.1 Following compliance with the Government Connect Code of Connection (CoCo) the Council was connected to the Government Connect Secure Extranet (GCSx) on 1 October 2009. This facility allows staff to securely send Council information up to RESTRICTED level to other public sector partners.

5.2 Compliance with the CoCo required rigid enforcement of the Council ICT Security Policy and a number of changes to the configuration of staff computers were made. These related to the locking down of user administration rights and internet browser settings, and the use of automatic e-mail previewing. This ensures compliance with sections 8.1 and 8.2 of the ICT Security Policy, relating to the configuration of devices and use of approved software.

5.3 These changes were implemented on 30 September 2009.

5.4 Further steps will be required to maintain compliance with Government Connect requirements which are subject to an annual audit.

6 SIGNIFICANT CHANGES TO THE POLICY

6.1 In the attached ICT Security Policy, the following changes have been made in italic text.

6.2 Third party access to Council ICT facilities (page 7, paragraph 6.4)

This amendment covers instances where other organisations, predominantly system suppliers, require remote access to the Council network to provide support or maintenance services. Granting such access must be done in a formal, secure way, with the approval of the relevant Council officer and only upon agreement that the third party will uphold the requirements of the Council ICT Security Policy and associated Codes of Practice.

6.3 Access to the Council ICT infrastructure and systems by staff of partner organisations and contractors (page 7, paragraph 6.5)

Checks to verify an individual's identity are made when recruiting Council staff. Access to Council ICT facilities is, however, regularly required by individuals who are not employees of Wirral Council. Consequently, confirmation must be sought by the Council officer authorising the access that equivalent identity checks have been performed on non-Council workers.

6.4 Corporate back up procedures (page 10, paragraph 9.1)

Internal Audit recommended that the ICT Security Policy is updated to clarify that corporate backups taken by IT Services are for business continuity purposes only.

6.5 Additional security incident types (Appendix 1, page 16, paragraph 2.4).

Two further examples of ICT security incidents have been added to the list.

6.6 The procedure 'Internet Misuse – Investigation Process' (Appendix 1, page 20, paragraph 5).

The list of IT Services officers to be contacted in the event of internet misuse has been amended.

6.7 Use of Mobile Devices – Things You Must Not Do.

The list has been amended to no longer prohibit international phone calls and text messages from Council provided mobile phones as they do not present a security risk.

6.8 Access to system accounts by an Investigating Officer during a disciplinary investigation or by a line manager for business continuity purposes (Appendix 4, pages 32-33).

An addition to the Use of Internet and Electronic Mail Facilities Code of Practice – Employees has been made to cross reference to the Council Discipline Policy. This refers to Investigating Officers during a disciplinary process being granted access to an individual's system accounts with permission from the appropriate Head of Service.

Additionally a line manager may need to access a member of staff's accounts for business continuity purposes if, for example, the individual is on sick leave. Again permission must be obtained from the appropriate Head of Service.

7 SUMMARY

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

8 FINANCIAL AND STAFFING IMPLICATIONS

8.1 There are no financial or staffing implications arising from this report.

9 EQUAL OPPORTUNITIES IMPLICATIONS

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

10 HUMAN RIGHTS IMPLICATIONS

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

11 LOCAL AGENDA 21 IMPLICATIONS

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

12 COMMUNITY SAFETY IMPLICATIONS

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

13 PLANNING IMPLICATIONS

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

14 LOCAL MEMBER SUPPORT IMPLICATIONS

14.1 The ICT Security Policy applies to all Members of the Council.

15 BACKGROUND PAPERS

15.1 Government Connect Code of Connection and Guidance.

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

15.3 Local Government Data Handling Guidelines.

16 RECOMMENDATION

16.1 That the amended Information and Communication Technologies Security Policy be agreed.

IAN COLEMAN
DIRECTOR OF FINANCE

FNCE/140/10