WIRRAL COUNCIL

CABINET

13 OCTOBER 2011

SUBJECT:	INFORMATION AND COMMUNICATION TECHNOLOGIES SECURITY POLICY
WARD/S AFFECTED:	ALL
REPORT OF:	DIRECTOR OF FINANCE
RESPONSIBLE PORTFOLIO HOLDER:	COUNCILLOR STEVE FOULKES
KEY DECISION?	NO

1.0 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 2 September 2010.

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

2.0 RECOMMENDATION

2.1 That the amended ICT Security Policy be agreed.

3.0 REASON FOR RECOMMENDATION

3.1 The ICT Security Policy must be regularly updated to reflect constantly evolving threats to Council information and ICT assets.

4.0 BACKGROUND AND KEY ISSUES

4.1 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

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

- 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 Strategic Change Programme,
- the requirements of Government Connect, which enables the secure exchange of data with public sector partners.
- the Big Society initiative

4.3 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.

4.4 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 file servers and storage systems
- multi-function devices, printers, faxes and other reprographic equipment
- network communications
- software.

Changes to the Policy

4.5 The changes to the ICT Security Policy are in italics. The majority are minor changes, including updated telephone numbers, internet hyperlinks and references within the document.

4.6 The more significant changes are as follows:

4.7 Users' Personal Data, paragraph 9.2

This new paragraph refers to the use of Council devices and fileservers on the network to store users' personal data and files – ie: data not being used to perform Council business. This can include digital photographs, digital music and videos. Council ICT facilities should not be used in this way. Users' personal data takes up storage space on the fileserver and can impact on performance.

4.8 Forwarding of Council emails to personal email accounts, paragraph 12.4

This amendment clarifies the issue of manually forwarding Council emails to personal email accounts. Council emails containing information classified as PROTECT or higher should not be forwarded to personal email accounts. If a user has a requirement to access Council emails or files remotely they should be provided with the secure means to do so. This can be arranged via the IT Services Helpdesk.

4.9 Reporting an Information/ICT Security Incident, Appendix 1

The procedures governing the Council response to ICT security incidents have been amended and now refer to information / ICT security incidents. This is to clarify that any incident affecting the confidentiality, availability or integrity of Council information should be reported, whether ICT is involved or not.

4.10 Information Classification: Government Protective Marking Scheme (GPMS), Appendix 2

The table in Appendix 2, paragraph 1 has been updated to reflect current Government guidance.

The table in paragraph 2.4 has also been updated. This now states that whilst information classified as PROTECT may be transmitted across public networks, such as the internet, or via fax, secure email facilities should be used if they are available.

4.11 Use of Mobile Devices & Removable Media, Appendix 3

The distinction between mobile devices and removable media has been clarified. Mobile devices are portable devices with data processing and storage capabilities. Examples include laptops, tablet PCs, Personal Digital Assistants, Smartphones and mobile phones.

Removable media refers to storage media which can be removed from a device, such as a computer, without the need to power the device off. This includes optical media, such as CDs/DVDs, memory cards, USB datasticks and external hard drives.

4.12 Use of Internet, Email and Telecommunications Facilities Code of Practice – Employees, Appendix 4

This has been updated and renamed to incorporate use of Council telecommunications facilities. The Code of Practice now confirms that use of the Council telephony system is for business purposes and that excessive personal use, publication of a Council telephone number for private use and use of offensive language is unacceptable.

It also clarifies that telephone calls made to the Call Centre are recorded for training and quality assurance purposes, and that such records of communications constitute a lawful interception of a communication under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

4.13 The document also confirms that excessive personal use of the internet, which could impact on employees' ability to fulfil the duties of their role, is unacceptable. As per minute 77 from the Executive Board meeting on 19 June 2006 use of the Internet should be kept to an absolute minimum between the hours of 9.00am and 5.00pm.

5.0 RELEVANT RISKS

5.1 The updates to the ICT Security Policy, as outlined above, will ensure that current and emerging threats to the security of Council information and information systems are appropriately managed.

6.0 OTHER OPTIONS CONSIDERED

6.1 No other options were identified.

7.0 CONSULTATION

7.1 The ICT Security Policy has been amended following consideration by the Information Strategy Group, the Information Manager and Internal Audit.

7.2 The updated Use of Internet, Electronic Mail and Telecommunications Facilities Code of Practice – Employees at Appendix 4 has, in addition to the above, been approved by Human Resources and Legal Services.

8.0 IMPLICATIONS FOR VOLUNTARY, COMMUNITY AND FAITH GROUPS

8.1 The ICT Security Policy must be adhered to by all users of Wirral Council ICT systems. This applies to third parties which may include voluntary, community and faith groups.

9.0 RESOURCE IMPLICATIONS: FINANCIAL; IT; STAFFING; AND ASSETS

9.1 There are no resource implications.

10.0 LEGAL IMPLICATIONS

10.1 There are no legal implications.

11.0 EQUALITIES IMPLICATIONS

11.1 There are no equalities implications.

11.2 Equality Impact Assessment (EIA)
(a) Is an EIA required? No

12.0 CARBON REDUCTION IMPLICATIONS

12.1 There are no carbon usage implications.

13.0 PLANNING AND COMMUNITY SAFETY IMPLICATIONS

13.1 There are no planning or community safety implications.

FNCE/209/11

REPORT AUTHOR: **Geoff Paterson**
Head of IT Services
telephone: (0151) 666 3029
email: geoffpaterson@wirral.gov.uk

APPENDICES

ICT Security Policy – September 2011

REFERENCE MATERIAL

SUBJECT HISTORY (last 3 years)

Council Meeting	Date
Cabinet – Agenda item 6 – Information and Communication Technologies Security Policy – Review	2 September 2010
Cabinet – Agenda item 27 - Information and Communication Technologies Security Policy	23 July 2009
Cabinet – Agenda item 4 - Information and Communication Technologies Security Policy	10 December 2008