REPORT TO CORPORATE RESOURCES OVERVIEW & SCRUTINY COMMITTEE

PORTFOLIO AREA: Learning & Development

Date of Meeting: **4 September 2008**

Public

Key Decision: **No** **Recorded in Forward Plan:** **No**

Inside Policy Framework

Title: **ICT Security Policy**
Report of: **Director of Corporate Services**
Report reference: **CORP44/08 – ICT Strategy Update**

Summary:

The Executive has referred this report to Corporate Resources Overview and Scrutiny for scrutiny. It contains the ICT Security Policy which they are considering adopting and recommending to Council.

Recommendations:

1) The Corporate Resources Overview and Scrutiny Committee are asked, after scrutinising the ICT Security Policy, to make such comments back to the Executive as they feel appropriate.

Contact Officer: John Nutley **Ext:** x7250

REPORT TO EXECUTIVE

PORTFOLIO AREA: Learning & Development

Date(s) of Meeting:	**Executive 26-August-2008** **Corporate Resources Overview & Scrutiny 04-September-2008** **Executive 22-September-2008**

Public

Key Decision: **Yes** **Recorded in Forward Plan:** **No**

Inside Policy Framework

Title: **Information and Communication Technology (ICT) Security Policy**

Report of: **Director of Corporate Services**

Report reference: **CORP44/08 – ICT Security Policy**

Summary:

This report proposes a new ICT Security Policy for the Council.

Recommendations:

1) The Executive is asked to:-

i) Consider the ICT security policy and identify any issues for further consideration.

ii) Refer the security policy to Corporate Resources Overview and Scrutiny Committee on 4th September for their comments back to the Executive 22nd. September.

Contact Officer: John Nutley **Ext:** 7250

1. BACKGROUND INFORMATION AND OPTIONS

1.1 A number of audit reports on Council systems have identified that the Council's current Information and Communication Technology (ICT) Security Policy is out of date.

1.2 This report formally presents a new ICT Security policy for the Council to adopt.

1.3 The policy is presented as a number of security principles that are to be adopted. It will be supported by a number of annexes that provide more detailed guidance in specific areas.

1.4 The policy principles are considered to form the fixed basis of the policy with the annexes being updated and added to on a regular basis as circumstances change. The annexes are in various stages of completion and it is anticipated will all be prepared and published by November.

1.5 The Senior Management Team and the Information Systems Group have considered the policy. Internal Audit was also asked for their comments on the policy.

1.6 Following adoption a communications exercise will be undertaken to ensure all staff and Members are aware of their responsibilities under the Policy.

2. RECOMMENDATIONS

Recommendations:

The Executive are asked to:-

i) Consider the ICT security policy and identify any issues for further consideration.

ii) Refer the security policy to Corporate Resources Overview and Scrutiny Committee on 4th September for their comments back to the Executive 22nd. September

3. REASONS FOR RECOMMENDATIONS

The approval of the ICT Security Policy formalises the good practice already employed by ICT users within the Council. It gives guidance to those who use the Council's ICT systems and authority to those charged with monitoring their use.

4. CONSULTATION

4.1 Consultation to Date

The Information System Group, which is attended by delegates from all Directorates, has approved the Policy.

Senior Management Team have also reviewed the policy.

4.2 Consultation proposed.

After adoption by the Council, all staff and Members will be reminded of their responsibilities under the Policy.

5. IMPLICATIONS

- Staffing/Resources – None
- Financial – None
- Legal – None
- Corporate – Once approved employees and members will be required to adhere to the policy and guidelines.
- Risk Management – The production of the policy and guidelines will improve the internal control arrangements of the Council as production of this policy is a key action in the Code of Corporate Governance approved by Council in June 2008.
- Equality Issues – None
- Environmental – None
- Crime and Disorder – None
- Impact on Customers – None

ANGELA BROWN
Director of Corporate Services

Contact Officer: John Nutley Ext: 7250

Information & Communications Technology (ICT)

Security Policy

Security Policy Principles

Objectives:

While recognising the importance of prompt access to accurate information within the Council there is a critical need to:

- Ensure the uninterrupted functioning of those manual and automatic information systems and information networks crucial to the Council's operation.
- Prevent the unauthorised use of information and information systems.
- Prevent the intentional or unintentional destruction of information.
- Ensure that staff, members and relevant third parties have access only to the information they require to undertake their duties.
- Minimise the extent any such incident should it arise.

Definitions:

The generic term of "systems" covers all computer software, computer hardware, data and voice networks, telephony and mobile telephone equipment.

Scope:

The Policy will cover all the Council's systems and the data stored, used by and/or transmitted by these systems.

All partners and contractors of the Council who require access to our systems will also be required to adopt this policy and demonstrate their compliance through independent audits.

Exclusions:
There are no Council systems excluded from this policy.

Policy Principles:

1. Systems are only available to those so entitled in a stipulated manner, at a stipulated time and at stipulated places.

2. Systems will be reliable, accurate and current and have not been altered or damaged due to faults in hardware, software, natural disasters or as a consequence of unauthorised human action.

3. Systems will be available and usable within a suitable time frame considering the nature of operations to authorised users.

4. Systems will be designed to ensure data and information systems cannot be used without permission.

5. Access to systems will be given at the least privilege level practical.

6. Systems will exist to ensure that documentary proof exists such that no party to a transaction or transfer can ever subsequently dispute his/her part therein.

7. The controls put in place to deliver these principles will be subject to a verifiable, independent audit.

Roles:

The ICT Unit will have the responsibility for both maintaining this policy and for its implementation.

The IT Security Specialist will have responsibility for the on-going identification and rectification of vulnerabilities to the Council's systems.

The internal Audit Team will have responsibility for ensuring timely and effective audits are undertaken at regular intervals. The results of these audits will be reported to the Audit Committee and the Information Steering Group (ISG)

The Information Steering Group (ISG) will be responsible for the approval of all Annexes to the Policy. In addition to ensuring that all ICT projects have given consideration to this policy before their approval.

Capital Projects Board will be responsible for identifying any project that has IT security implications and ensuring that these have been considered by the ISG before approval is given.

Members and staff will be responsible for their adherence to the policy.

Approach:

Using these principles a number of detailed guidelines will be developed and be presented as Annexes to the policy. These will include, but not exclusively, the following functional areas:-

- Securing Hardware, Peripherals and Other Equipment
- Controlling Access to Information and Systems
- Processing Information and Documents
- Purchasing and Maintaining Commercial Software
- Developing and Maintaining In House Software
- Combating Cyber Crime
- Complying with Legal & Policy Requirements
- Planning for Business Continuity
- Addressing HR Issues relating to Information Security
- Controlling on-line & e-security Information Security
- Dealing with Premises related consideration
- Detecting and responding to Information Security Incidents

These Annexes will be regularly updated inline with new legislation, industry best practice and the evolution of threats to our systems.

Where appropriate the Council will achieve accreditation, i.e. Payment Card Industry Data Security Standard (PCI DSS), Government Connect Code of Conduct (CoCo), for it systems to demonstrate both the commitment to this policy and the achievement of nationally recognised standards which will give confidence to the general public and our partners in our ability to deal with their information in a secure and appropriate manner.

Training will be provided for all users of our systems to raise awareness of the need for security, their responsibilities and the guidelines to be followed. In additional specialist training will be provided to the Council's Facilities Management team to ensure the need for physical security is included in all building projects.

Through the staff appraisal process and Team Improvement Reviews (TIR) all IT staff will have the appropriate knowledge and skills to implement this policy. A specific IT security role has already been identified and included in the relevant job description. The current and any subsequent post holder will be required to obtain nationally recognised IT security qualifications, i.e. Certified Network Security Professional (CNSP).

Given specialist nature of IT security auditing and the difficulty in justifying such a post within the Council, the Head of Audit will identify suitability qualified individuals or organisations to undertake detailed security audits. The audit of IT security will also be included in the annual audit plan.

All hardware, software and services procured by the Council will comply with the relevant security standards. This will be achieved by the inclusion in all procurement documents of this requirement by the Council's Procurement team.

Related ICT Policies:

The ICT Strategy of the Council will include reference to this policy. In addition adequate resources will be allocated to ICT security in the annual ICT Service Plan.

Related Council Policies:

The following Council's policies will include references to this policy:

- Corporate Risk Register
- Corporate Business Continuity Plan.
- Corporate Procurement Policy