REPORT NO. 3

REPORT TO THE SCRUTINY PANEL for PEOPLE

2nd February, 2012

Status:	**For review**
Title:	**Update to ICT Security Policy**
Originator:	**Chris James, ICT Manager**
Where from:	**Executive**
Where to next:	

Objective: To undertake the regular review of the corporate ICT Security Policy and also to update it in line with recommendations arising from audit reports.

1. Outcome sought from Panel

1.1. For the Scrutiny Panel – People to review and consider changes to the ICT Security Policy.

2. Background

2.1. This reviewed current ICT Security Policy was approved by the Executive on 7th November, 2011.

2.2. The current policy states that it will be reviewed on an annual basis.

2.3. The current policy also states that it will be reviewed independently. The policy is regularly reviewed by both internal and external auditors (the Audit Commission are currently performing an “IT risk assessment – refresh”).

2.4. Recent ICT Health Checks and Penetration Tests performed by an external security company (NTA Monitor) have highlighted issues requiring attention.

2.5. Physical security and care of equipment whilst offsite required clarifying.

2.6. Accompanying policies for e-mail and internet usage needed to be refreshed.

3. Points for discussion

3.1. A recent set of security checks highlighted the need to include a statement about the need for HDC staff to challenge unknown personnel within the premises and any attempted access to systems or equipment.

3.2. Overnight storage of loan equipment: recommendations have been added to protect equipment from extremes of temperature.

3.3. E-mail security procedure statements have been updated and clarified.

3.4. The E-mail and Internet Usage Policies are referenced by the ICT Security Policy and needed to be reviewed at the same time. These associated policies have been refreshed by reviewing, re-formatting (to share a common look and feel as well as version number with the Security Policy) and applying minor updates where required.

3.5. Members are asked to consider the changes to the ICT Security Policy and suggest any changes for consideration in the next policy review.

4. Equality Impact Assessment Implications/Outcomes (attach completed EIA)

4.1. An Equality Impact assessment has previously been undertaken on the ICT security Policy and the suggested changes do not call for any additional activities to be carried out.

5. Impact on Communities

5.1. The proposed policy is designed to safeguard personal data.

6. Legal Issues

6.1. The requirement to safeguard personal data is a legal requirement.

7. Resource Issues

7.1. Changes to the ICT Security Policy have already been communicated to officers and elected members using existing resources.

8. Community Safety Implications

8.1. The proposed policy is designed to safeguard personal data.

9. Carbon Management Implications

9.1. The revised ICT Security Policy will be made available electronically to reduce the use of paper.

10. Risk Management Implications

10.1. Accepting the proposed changes to the ICT Security Policy will minimise risk to the Council.

11. Consultation

11.1. Consultation has not been sought for the minor changes made in this iteration of the security policy. No changes were made within the supporting policies either; the refresh of these documents was cosmetic.

12. Background Papers

12.1. None

Previous report(s):

Information Issued Under Sensitive Issue Procedure: N

Appendices: *list any appendices here including title and filename in brackets (e.g. Performance Data 2010 (perfdata.doc).*

A. ICT Security Policy

B. ICT E-mail Usage Policy (for reference)

C. ICT Internet Usage Policy (for reference)