PAPER NO. 2

REPORT TO THE EXECUTIVE MEETING OF 07/11/2011

Status:	**Decision**
Title:	**Annual Review of ICT Security Policy (Including a refresh of associated E-mail and Internet Usage Policies)**
Originator:	**Chris James, ICT Manager**
Where from:	
Where to next:	**Implementation**

---

1 Purpose of the Report

1.1 To undertake the annual review of the corporate ICT Security Policy and also to update it in line with recommendations arising from audit reports

2 Recommendations:

2.1 To approve the ICT Security Policy as attached at Appendix A.

3 Summary of Reasons for the Recommendations

3.1 The current ICT Security Policy was approved by the Executive on 16th August 2010.

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

3.3 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.

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

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

3.6 The E-mail and Internet Usage Policies are referenced by the ICT Security Policy and need 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.

4 Impact on Communities

4.1 The proposed policy is designed to safeguard personal data.

5 Key Facts

5.1 The Council undertakes security vulnerability assessments by our own staff as well as annual network penetration and ICT Health Check testing by a third party. The annual Security Policy renewal provides an opportunity to include any additional requirements highlighted by these assessments such as the social engineering issue (item 3.3).

.

6 Legal Issues

6.1 The requirement to safeguard personal data is a legal requirement. Compliance with PCI DSS is also a legal requirement.

7 Resource Issues

7.1 Changes to the ICT Security Policy will be communicated to officers and elected members using existing resources.

8 Equality Impact Assessment Implications/Outcomes

8.1 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.

9 Impact on the Organisation

9.1 It is important that the Council has a robust ICT Security Policy in place to safeguard both ICT equipment and data. The ICT Security Policy also contains restrictions and practices which are required by the Government Security Standard Code of Connection (CoCo) that the Council must adhere to in order to exchange data with other public sector organisations, such as Department for Works and Pensions.

10 Community Safety Implications

10.1 The proposed policy is designed to safeguard personal data.

11. Carbon Management Implications

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

12. Risk Management Implications

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

13 Consultation

13.1 This is a minor update only and subsequently consultation has only taken place within ICT and with the Council's Management Board.

14 Options Considered

14.1 It is necessary for The Council to have an ICT Security Policy to ensure it meets legal requirements regarding data security.

15 Background Papers

15.1 None.

Previous report(s): ***ICT Security Policy – Executive meeting of 16th August August 2010.***

Information Issued Under Sensitive Issue Procedure: N

Ward Members Notified: N

Appendices:

A. ICT Security Policy.doc

B. ICT E-mail Usage Policy.doc

C. ICT Internet Usage Policy.doc