WARWICK DISTRICT COUNCIL	**EMPLOYMENT COMMITTEE**	**Agenda Item No.**

Title	ICT – ISCP 2009 REPORT
For further information about this report please contact	TY WALTER
Service Area	CUSTOMER & INFORMATION SERVICE
Wards of the District directly affected	N/A
Is the report private and confidential and not for publication by virtue of a paragraph of schedule 12A of the Local Government Act 1972, following the Local Government (Access to Information) (Variation) Order 2006	NO
Date and meeting when issue was last considered and relevant minute number	N/A
Background Papers	SMT 19th August 2009

Contrary to the policy framework:	~~Yes~~/No
Contrary to the budgetary framework:	~~Yes~~/No
Key Decision?	~~Yes~~/No
Included within the Forward Plan? (If yes include reference number)	~~Yes~~/No

Officer/Councillor Approval

With regard to officer approval all reports *must* be approved by the report authors relevant director, Finance, Legal Services and the relevant Portfolio Holder(s).

Officer Approval	**Date**	**Name**
Relevant Director	SMT Aug 2009	Andy Jones
Chief Executive	SMT Aug 2009	Chris Elliot
SMT / CMT	SMT Aug 2009	
Section 151 Officer	SMT Aug 2009	Mike Snow
Legal	SMT Aug 2009	Peter Oliver
Finance	SMT Aug 2009	Mike Snow
Portfolio Holder(s)		Les Caborn

Consultation Undertaken

Please insert details of any consultation undertaken with regard to this report.

Consultation and approved by ICT Steering Group

Final Decision?	**~~Yes~~/No**

Suggested next steps (if not final decision please set out below)

1. SUMMARY

1.1. The Information Security & Conduct Policy (ISCP) has existed in its current format for several years. It has been a single document encompassing all aspects of Information Security but, despite its title, has largely focused on ICT Security. The document is updated at least annually by ICT Services, although the formal consultation on the document is undertaken by Human Resources because it forms part of an employee's terms and conditions.

1.2. The Information Security Policy for 2009 has taken a significant departure from previous policies. The ISCP still remains, but the policy has been broken down into nine sub-policies. Although this was largely inevitable due to the growth of the policy, the major driver this year has been due to the council's need to meet central government's Code of Connection (CoCo).

2. RECOMMENDATION

2.1. Employment approve the Information Security and Conduct Policy 2009 and its associated sub-policies.

2.2. ICT Services identify an appropriate phased implementation plan for the policies and develop associated training material and staff awareness campaigns.

2.3. Service Area Managers should ensure that all their staff, especially those who are system owners, are appropriately trained and are aware of the practical application of these policies.

3. REASONS FOR THE RECOMMENDATION

3.1. The option not to have an up to date Information Security Policy would be contrary to the good governance of the Council and would expose the Council to significant risk through poor security practices.

3.2. Equally not making the policy amendments required to meet CoCo compliance, would impact the council's ability to deliver the Housing Benefits service.

4. ALTERNATVE OPTIONS CONSIDERED

4.1. Failure to update the Council's security policy to reflect the threats posed by new technologies and services could seriously impact service delivery (virus, hacking, data loss, etc) and the reputation of the council. Therefore, no alternatives were considered.

5. BUDGETARY FRAMEWORK

5.1. The work on the Information Security Policy, including changes to the infrastructure resulting from Code of Connection compliance, has been undertaken within existing budgets and resources.

6. POLICY FRAMEWORK

The Information Security and Conduct Policy supports the Council's Corporate Strategy by providing a secure environment under which 'Leading Edge' technology can be deployed to improve efficiency and public service quality

7. BACKGROUND

7.1. Early in 2008 the Department of Work and Pensions (DWP) notified all Local Authorities that Council Housing Benefit departments would no longer be able to access the DWP's Customer Information System (CIS), and other services which provided sensitive data, without a secure link from April 2009. The secure link, which the DWP mandated, was the Government Secure Extranet (GCSx)

7.2. The GCSx is a government accredited secure network for all local authorities in England and Wales. It enables the sharing of sensitive personal data and data protectively marked as RESTRICTED by central government.

In addition the GCSx provides:

- Secure access to central government applications and databases.
- Secure email exchange with central government, Police, NHS and other local authorities.
- Secure bulk-file transfer between local and central government.

7.3. To enable the Council to connect to the GCSx, the Council had to meet a minimum set of central government security standards set out in the Code of Connection (CoCo). The CoCo was defined by the Communications-Electronics Security Group (CESG) who forms part of the Government Communications Headquarters (GCHQ).

7.4. The CoCo has 91 standards or controls that the authority must meet. These controls vary in nature and range from how we configure our network at a technical level, to how we send and receive e-mails. It has taken ICT Services eleven months and numerous submissions to meet the requirements of the CoCo. At the point that Warwick District Council received CoCo approval from CESG (March 2009), over 300 of the 410 councils in England and Wales had still not met the standard.

7.5. Although the CoCo has put major technical constraints on how ICT is configured within the Council, the CoCo also puts constraints on how technology is used. From a governance perspective these constraints need to be documented and reflected in the Council's security policies. Primarily it has been this driver which has resulted in the ISCP being sub-divided.

7.6. These constraints are not unique to Warwick District Council, but apply to all 410 English and Welsh authorities. Therefore, the WMLGA formed a group to review the security requirements of the CoCo and to produce a number of template policies. ICT Services has taken these policies and modified them, where possible, to meet the needs of Warwick District Council.