

COMMITTEE: STANDARDS Ref No: ST/08/01

DATE: INFORMATION SECURITY AND ICT
ACCEPTABLE USAGE POLICIES

REPORT AUTHOR: HOWARD GASKIN, ICT INFRASTRUCTURE
MANAGER

DIRECTOR: TRACEY LEE

Short description of report content and the decision requested:

This report (ICT Security Policy) is a standard ICT policy as recommended by industry best-practice and required by internal/external Audit. With the addition of the appendices (Acceptable usage policies) it is also suitable as a replacement for the existing 'IT code of good practice' (last revised in 2006).

It is generally based upon a recent policy from St Edmundsbury, which was significantly reviewed after their recent loss of laptop incident. The Policy also includes recent advice given to IBC Managers following the DWP data disk loss and previous advice, given by Finance, on the private use of IBC telephones.

The request is that this report be considered for adopting as council policy.

This report has been prepared by Howard Gaskin, Tel: 01473 433891 - Email: howard.gaskin@ipswich.gov.uk

This report was prepared after consultation with:

Directors Team, Audit, Legal and was put out for comment to all employees (including Unison).

The following policies form a context to this report:

(all relevant policies must also be referred to in the body of the report)

ICT Code of good practice (2002) & (2006)

This report is not a key decision included in the Forward Plan

LIST OF BACKGROUND PAPERS AS REQUIRED BY LAW

(papers relied on to write the report but which are not published and do not contain exempt information –

OTHER HELPFUL PAPERS

(papers which the report author considers might be helpful – this might include published material)

1. ICT code of good practice (2002) & (2006)
2. Data Protection Act, 1998
3. Copyright Designs and Patents Act, 1988
4. Computer Misuse Act 1990
5. Freedom Of Information Act 2000

1. Introduction

- 1.1 The purpose of this report is to replace the existing ICT code of good practice with a more robust policy more suited to the increased threat and awareness of ICT security issues.

2. Background

- 2.1 The previous ICT Code of good practice was adopted in 2002 it was reviewed in 2006, but not formally adopted.
- 2.2 Recent national security issues have highlighted the need for a more robust and enforceable policy – this has also been a request from Internal and External Audit.
- 2.3 The policy covers the following issues:
- To ensure that all of the Council's assets, users of ICT, data and equipment are adequately protected on a cost-effective basis against any action that could adversely affect the ICT services required to conduct its business.
 - To ensure that users are aware and fully comply with all relevant legislation.
 - To create and maintain within all service areas, a level of awareness of the need for ICT security to be an integral part of the day to day operation, so that all staff understand the need for ICT security and their own responsibilities.

3. Policy Context

- 3.1 The security policy is relevant to all ICT services irrespective of the equipment or facility in use and applies to:
- All employees, Councillors and agents;
 - Employees and agents of other organisations who directly or indirectly support or use the ICT services;
 - All use of ICT throughout the Council and at home or in other organisations when engaged on Council business.

4. Performance Monitoring

- 4.1 This policy should be reviewed annually or more frequently if a specific new ICT threat arises.

5. Risk Management

Risk	Impact of risk, if it occurred* (Scale of 1-4) 1 – Catastrophic 4 - Negligible	Probability of risk occurring* (Scale A-F) A- Very likely F - almost impossible	What is the council doing (or what has it done) to avoid the risk or reduce its effect?
-------------	---	--	--

That the policy does not cover all ICT security issues	2	E	The policy is based upon similar works by other authorities and has been created after consultation with Legal and Audit sections.
That the policy becomes outdated or does not properly address new security threats.	2	C	The policy should be reviewed annually or when a new ICT security threat arises.

6. Environmental Impact Assessment

6.1 There is no environmental impact directly associated with this report.

7. Equalities and Diversity Implications

7.1 Sections of this policy (email/internet usage) are directly concerned with the safeguarding of the Council's equalities and diversity policies.

8. Financial Considerations

8.1 There are no direct financial implications associated with this report other than officer time to prepare and maintain the report.

9. Conclusions

9.1 This report aims to ensure that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level which is appropriate for the Council's needs.

10. Recommendation:-

10.1 That the Committee notes the report and make its observations to the ICT Infrastructure Manager as to any requirement for further action.