Doncaster
Metropolitan Borough Council

Information Security Policy

V2.2

Information Security Policy

Contents

This policy shall be reviewed annually to ensure it remains appropriate.

Version	Date of Revision	Amended by	Reasons
1.0	April 2006	C Whitechurch	Initial version
2.0	July 2007	C Whitechurch	Amended to incorporate references to new acceptable use and technical policies..
2.1	July 2007	C Whitechurch	Added hyperlinks to all relevant legislation and policies and changed format to DMBC Standards.
2.2	November 2010	M Meakin	Updated text and hyperlinks and changed format to include standard DMBC format. Minor amendments to reflect changes in directorate / service names.

1. Introduction

The information held on the Council's information systems is a vital asset. The availability, integrity and confidentiality of this information plays an essential role in ensuring that the Council can maintain and improve its operational efficiency, take correct decisions, comply with legislative requirements and protect the Council's image. The Council's increasing dependence on information systems means that it is becoming more vulnerable to security threats, including sabotage, vandalism, fraud, accidental damage or loss, virus infection, unauthorised disclosure or interception.

Information exists in many forms; printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

All Council Officers and Members need to be made aware through induction or job training of the important part they play in ensuring that all of the Council's systems are protected and are aware of the parts of the policy relevant to their post.

2. Scope, Definitions and Objectives

The purpose of Information Security is to ensure business continuity and to minimise business damage, by preventing and minimising, the impact of security incidents and weaknesses. Information Security Management enables information to be shared appropriately, whilst ensuring the protection of information and computing assets. Information Security Management has three basic components:

(i)	confidentiality or privacy:	protecting sensitive information from unauthorised disclosure or intelligible interception.
(ii)	integrity:	safeguarding the accuracy and completeness of information and software.
(iii)	availability or resilience:	ensuring that information and vital services are available to users when required.

3. Statement of Management Intent, Roles and Responsibilities

The Council recognises the vital importance of Information Security in ensuring the protection of its information and computing assets. The Council is committed to ensuring that rigorous Information Security Policies and Controls are developed and maintained to achieve this protection.

This policy follows the ISO27001 guidelines on Information Security and as such it is important to identify all relevant stakeholders and to describe their responsibilities: -

Corporate Leadership Team	To endorse and support the Information Security Policy.
ICT	To develop and maintain Information Security Policies and controls. To investigate, procure, install and maintain technical solutions for security weaknesses where appropriate.
Audit Services	To undertake periodic reviews of information security and adherence to the policy throughout the Council.
People and Performance Improvement	To provide professional advice regarding Information Security Policies and Controls.
Legal Services	To provide professional advice regarding Information Security Policies and Controls.
Directorates	To adhere to the Information Security Policy. To develop and maintain business continuity plans for their environments.
Members, Council Officers, Contractors and Third Party Providers	Information security is the responsibility of every Member, Council Officer, contractor and third party provider and all are expected to fully comply with all Information Security Policies and Controls.

4. Legal and Regulatory Obligations

Individuals will be expected to comply with all procedures relevant to the statements below:

The Council will implement procedures to ensure that, so far as is practicable:

- The design, operation and use of Information Security/ICT systems comply with all relevant statutory and contractual security requirements

- Copyright material is not copied without the owner's consent, all software used on Council computers is correctly licensed and that unauthorised copying of proprietary or Council software is detected and remedied.

- Important Council records are safeguarded from loss, destruction and falsification. (The specific procedures to be followed for retention, storage, handling and disposal of Council records and information will be outlined in further policies).

- Applications handling personal data (on individuals) comply with Data Protection Legislation and principles and that personal data is kept secure from unauthorised access, alteration, disclosure, loss or destruction.

- Council Information Security/ICT facilities must only be used for authorised purposes. The Council may monitor or investigate usage of IT facilities and any person found using Information Security/ICT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary proceedings.

The Council is required to demonstrate compliance with the following pieces of legislation (this list is not exhaustive):

- The Copyright, Design, and Patents Act 1988
- The Computer Misuse Act 1990
- Defamation Act 1996
- The Data Protection Act 1998
- The Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Local Government Act 1972 & 2000

Also included are the Council's Policies and Guidelines:

- Corporate Whistleblowing Policy
- Disciplinary Procedure
- Code of Conduct
- Emergency Planning
- Data Protection Policy
- E-mail Usage Policy

- Internet Usage Policy
- Acceptable Use Policy
- Technical Security Policy
- Information Sharing Protocol

5. Strategic Approach and Principles

Information Security Education and Training

All users of Information Security/ICT facilities will be given adequate security education and technical training.

Virus Prevention and Detection

Virus prevention, detection measures and appropriate user awareness procedures will be implemented across all appropriate environments. All users must report virus infection as soon as possible to the ICT Help Desk.

Business Continuity Planning

Business continuity plans will be created and maintained for all environments, in order to maintain operations following failure or damage to vital services/facilities.

Access Controls

Access to Information Security/ICT facilities and data will be controlled on the basis of business requirements.

6. Risk Management

Before any new ICT system is implemented a risk assessment must be carried out in order to assess the security risk to the Council.

All contractors/organisations that provide a service to the Council must be subject to a security risk assessment before entering in to the contract to ensure that all adequate controls and procedures are in place prior to the commencement of the service.

All employees and third party providers must report any security incidents/breaches to ICT who will initiate an appropriate response to the incident in question. Please see the Security Incident Policy and Emergency Security Incident Procedure for guidance.

- Security Incident Policy
- Emergency Security Incident Procedure
- Emergency Security Incident Working Group

7. Actions in the Event of a Policy Breach

A breach is an event that has, or could have, resulted in loss or damage to Council assets, or an action that goes against the Council Information Security procedures and should be logged through the ICT Help Desk.

The Council may monitor or investigate usage of IS/IT facilities and any person found using these facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary proceedings in line with the Acceptable Use Policy.