Alternative Formats

This document is available in large print, Braille, audio tape, electronic formats such as CD, or in a different language. Our website is ReadSpeaker enabled. For a copy please contact the Policy and Performance Team at the Council using the following options:

Phone: 01529 414155 (main switchboard) or 01522 699699 (if calling from a Lincoln number)

Minicom: 01529 308088

Fax: 01529 413956

Web: www.n-kesteven.gov.uk

Email: equality@n-kesteven.gov.uk

Corporate Information Manager
North Kesteven District Council
Kesteven Street
Sleaford
Lincolnshire
NG34 7EF
Introduction

Information is an important asset and of significant value to North Kesteven District Council. The Council must protect its information from threats, internal and external, deliberate or accidental, that could disrupt its work or infringe the rights of employees or customers.

Information security involves the protection of information for:

- **Confidentiality**: making sure that information is accessible only to those authorised to have access
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods
- **Availability**: ensuring that authorised users have access to information and associated assets when required.

All information created or processed on behalf of the Council is regarded as being owned and accessible by it as part of the Council’s ‘business record’.

This Policy focuses on all types of information and security including:

- information systems;
- paper records;
- microfiche, visual and photographic materials e.g. CCTV, slides;
- spoken conversation, including voicemail and recorded conversations; and
- technology used to hold, process, transfer and transmit the Council’s information e.g. memory sticks.

The Policy applies throughout the lifecycle of the information from creation through storage and use to disposal. All the controls required will be effective and appropriate; offering adequate protection without unnecessary expense or intrusion.

Information Security Policy Statement

**Aim of the Policy**

The overall aim of this Policy is to reduce the risks, from whatever source, to the security of the Council’s information and that of its customers and partners. By doing this, the Policy will minimise potential damage to the Council, its assets and its reputation, by preventing and reducing the impact of security incidents.

The Information Security Policy is in place to make sure that:

- the Council establishes a culture of care for information held by the local authority and immediately report any incidents of loss;
- information is only obtained when it is required;
- information owned or processed by the Council is protected against unauthorised access or use;
- Information and Communication Technology (ICT) equipment is protected from accidental or malicious damage;
- security risks are properly identified, assessed, recorded and managed;
- cost-effective safeguards are implemented to reduce security risks;
- appropriate monitoring and reporting processes are put in place to identify and act immediately upon breaches of information security;
- legal and regulatory requirements are understood and met; and
- information and training on information security is available and up-to-date.
Approach
This Policy is based on an industry standard framework and the ISO/IEC 27000 series the International Standards for information security management.

Application
This Policy applies to all employees, elected Members, contractors, agents, representatives and temporary staff working for or on behalf of the council.

Aspects of this Policy will be relevant to people the Council share information with, such as, voluntary organisations, agencies and partnerships, as part of the work of the council.

Roles and Responsibilities

Heads of Service shall maintain a high-level overview of data and information security.

The ICT Manager is the designated owner of the Information Security Policy and is responsible for providing direction for the management of information security.

Raising awareness of this policy shall be led by the ICT Team and is the responsibility of all Managers. All Managers are responsible for making sure that this policy is communicated within their service and that all their staff know about and understand their information security responsibilities.

It is everyone’s responsibility to make themselves aware of the content of this Policy and to adhere to it.

Breaches of the Policy
Breaches of this Policy are regarded as a disciplinary matter and, in the case of a member of staff, those classed as gross misconduct, may lead to dismissal. Breaches of this Policy by an elected Member are covered by the Member Code of Conduct and could be referred to the Standards Committee.

Any breaches, observed or suspected, of the ICT Security Policy must be handled in accordance with the Information Security Incident Management Policy.

Policy Implementation
This Policy will be made available to all employees (whether permanent or temporary), elected Members and partners/agents.

Risk Assessment, Treatment and Management

The Council shall provide protection to its information assets and systems where these assets are held, commensurate with their value and importance to the organisation.

Risks will be assessed and appropriate control measures put in place to reduce these risks.

So that appropriate control measures can be put in place before their implementation or use, the business sponsor or system owner will assess the Information Security risk of:

- all new information assets and systems; and
- modifications or development of existing systems.

Having identified the risks, appropriate measures will be adopted to make sure systems and information are secure.
There must be periodic reviews of the identified security risks and related controls, taking accounts of new threats and vulnerabilities, to determine whether current controls are still effective.

Audit can give an independent assurance on the controls implemented.

**Organisation of Information Security (the Framework)**

The strategic direction of the Council in matters of ICT and information security is towards full compliance with the International Standards ISO27000 Series.

The Council and its employees and agents shall abide by all United Kingdom and European legislation which is relevant to the security of its information. Relevant legislation includes:

- Common Law Duty of Confidentiality;
- Computer Misuse Act (1990);
- Copyright, Designs and Patents Act (1988);
- Data Protection Act (1998);
- Freedom of Information Act (2000);
- Human Rights Act (1998);
- Civil Contingencies Act (2004);
- Electronic Communications Act (2000);

Where relevant to local government the Council shall comply with the guidance contained in the National Information Assurance Strategy for Local Government. The current general version can be found at the Cabinet Office website:


**Information and ICT Asset Management**

**Responsibility for assets**

All assets (data, information, software and hardware) must be accounted for and have an owner. The owner shall be responsible for the maintenance and protection of the asset(s) concerned.

Documented rules will be established and maintained for the acceptable use of information and assets associated with information processing facilities.

**Information Classification**

All information assets should be classified and protected.

**People and Organisational Development**

Upon a change or termination of employment, clearly defined and assigned procedures must be followed at all times. These include the return of all council-owned assets and the revoking or amendments of the person’s access rights.

**Physical and Environmental Security**

Physical security and environmental conditions must be suitable to manage the risks to the area concerned. In particular critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls and protection for the infrastructure.

Information, including electronic information and printouts produced from computer systems, must be stored and used in accordance with the principles of the Data Protection Act 1998, any other legislation, council information and records management policies.
The Council recognises that employees, elected Members and agents may need access to Council information and systems from home or other remote locations. They also need to access information and communicate electronically using public networks, such as, the Internet. The following Policy documents provide information and guidance on accessing Council systems from outside the Council’s physical boundary and the acceptable use of the Internet and electronic communication services:

- Remote Working Policy
- Removable Media Policy
- Internet Acceptable Use Policy
- Email Policy.

**Communications & Operations Management**

Responsibilities and procedures for the management, operation and ongoing security and availability of all information processing facilities within, outside and between the Council and other partner or third party organisations must be established.

Information must be stored and destroyed in a controlled manner.

A Records Retention and Disposal Schedule must be implemented for all information holding systems both manual and electronic.

**Information and Systems Access Control**

Access to information and information systems must be driven by business requirements. Access shall be granted to employees, elected Members, contractors and third parties to a level that will allow them to carry out their duties and shall not be excessive of their role.

A formal user registration and de-registration procedure is required for access to all information systems and services. This must include amendments when employees change roles within the council.

Necessary controls will be put in place before connecting third parties to any council ICT facilities after approval by ICT.

**Information Systems and Technology Management**

Security is an integral part of information systems. Security risks and requirements must be identified at the earliest stage in the system development or acquisition cycle, along with controls to be implemented to mitigate the risks.

**Information Security Incident Management & Monitoring**

Information security incidents and weaknesses must be recorded and mitigating action taken in a consistent and timely manner.

All employees will be encouraged to report any security breach, actual or potential, without fear of recrimination.

All security incidents will be logged and investigated where appropriate.

Security incidents that result from a deliberate disregard of any security policy requirements may result in disciplinary action.

**Business Continuity Management**

Arrangements must be in place for the timely resumption of business information systems in the event of a failure in these systems or damage to them arising from a disaster.
Service continuity planning for the ICT systems will be carried out by the ICT Department, but the business areas will be responsible for the business continuity plans for the services they provide.

The purpose of the plan is to reduce, to an acceptable level, the actual or potential disruption caused by, among other things, failures of information security.

Disaster recovery arrangements will be tested at least annually and will be reviewed and updated as areas of business risk are identified and business continuity arrangements are developed.

**Compliance**
The design, operation, use and management of information systems must take into consideration all statutory, regulatory and contractual security requirements as well as organisational security policies and standards.

The security of information systems will be regularly reviewed and audited in order to ensure that they comply with security policies and standards.

The Information Security Framework must provide the necessary controls to maintain compliance with the following codes and standards.

**Policy Review**
This Policy will be formally reviewed every two years to ensure it continues to be relevant and current. In some circumstances it may be necessary to review this Policy more frequently in response to specific events.