ASKERN TOWN COUNCIL
Alexander House, High Street, Askern,
Doncaster DN6 0AB
Tel: (01302) 707252
Email: admin@askerntowncouncil.gov.uk
Website: www.askerntowncouncil.gov.uk

INFORMATION SECURITY POLICY

1. Introduction

1.1. Askern Town Council recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, the Council will facilitate the secure and uninterrupted flow of information, both within the Council and in external communications. the Council believes that security is an integral part of information sharing which is essential to corporate endeavour and the policies outlined below are intended to support information security measures throughout the Council.

2. Definition

2.1. For the purposes of this document, information security is defined as the preservation of:

- confidentiality: protecting information from unauthorised access and disclosure;
- integrity: safeguarding the accuracy and completeness of information and processing methods and
- availability ensuring that information and associated services are available to authorised users when required.

2.2. Information exists in many forms. It may be 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.

3. Protection of Personal Data

The council holds and processes information about employees, councillors, customers and other data subjects for administrative and commercial purposes. When handling such information, the Council, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the General Data Protection Regulation.

4. Information Security Responsibilities

4.1. The Council believes that information security is the responsibility of all members of the council and its staff. Every person handling information or using Council information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the Council.

4.2. This policy is the responsibility of Askern Town Council; supervision of the policy will be undertaken by the Clerk. Implementation of information security is managed through the Clerk and other designated personnel with security responsibilities in specified areas of the Council.

5. Compliance with Legal and Contractual Requirements

6.1. Authorised Use - Council facilities must only be used for authorised purposes. The Council may from time to time monitor or investigate usage of IT facilities and any person found using IT facilities for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

6.2. Access to Council Records - In general, the privacy of users' files will be respected but the Council reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and the Council policies and regulations, and the determine which records are essential for the Council to function administratively. Expect in emergency circumstances, authorisation for access must be obtained from the Clerk, or nominee and shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

7. Retention and Disposal of Information

7.1. All staff have a responsibility to consider security when disposing of information in the course of their work. All personal information shall only be retained for as long as it is necessary to complete the Council's business and should then be destroyed in line with Askern Town Council's Retention and Disposal Policy.

8. Reporting

8.1. All staff and other users should report immediately to the Clerk if:

- any observed or suspected security incidents where a breach of the Council's security policies has occurred,
- any security weaknesses in, or threats to, systems or services.

8.2. Software malfunctions should be reported to the Clerk.

9. Disclosure of Personal Information

In most circumstances members of the Council do not need to be aware of or hold personal information in order to carry out their duties, however, in circumstances where personal information does become available to them this policy applies.