STOTFOLD TOWN COUNCIL

INFORMATION SECURITY POLICY

Preamble

This policy has been drawn up to reflect the guidance contained in BS ISO/IEC 27001.

BS ISO/IEC 27001 is a standard based on years of practical security experience in real businesses. The main objective of the standard is to help establish and maintain an effective information management system.

It is important to be secure against outside threats.

Information does not mean just computer-stored data. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or electronically, or spoken in conversation.

Information security means preserving:

- **Confidentiality** – ensuring that information is accessible only to authorised users
- **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

Information security is achieved by implementing suitable controls on:

- Policies
- Procedures
- Organisational structures
- Software functions

Risks to Information Security

Threats to information security can be categorised into six groups:

- Fraud, including identity theft
- Fire, flood and other natural disasters
- Industrial espionage
- Computer viruses
- Data loss
- Loss of service

Security Policy

Information Security is very important to Stotfold Town Council.

The Town Clerk will be expected to undertake training on information security as appropriate from suitable sources such as Bedfordshire Association of Town and Parish Councils, Society of Local Council Clerks and other appropriate sources.

The Town Council will ensure that elementary precautions concerning computer viruses, etc, are in place to protect the Council's computers.

Town Council computers are password protected and all authorised users are instructed to keep these private.

Town Council computer records will be regularly backed up on to an independent drive and stored separate from other computer records, together with external back up via a cloud system.

All security problems will be reported to the Town Council and minuted accordingly. In the event of a serious incident, the Council Chairman will be notified immediately. In the event of a data breach, the Information Commissioners Office will be notified in accordance with current legislation.

The Town Council has a Data Protection Policy that is in accordance with current legislation.

This Information Security Policy will be reviewed on a three yearly basis by the Council.

Organisational security

The structure and function of the Town Council minimises the requirements for organisational security.

Where appropriate, the Town Council will seek external expert advice.

All new information-based projects and resources will be approved by the Town Council and expert advice will be obtained as necessary.

Asset classification and control

The Town Council maintains an inventory of information assets. Assets include the information itself, computers and software.

The inventory details the degree of sensitivity of the information, that they receive an appropriate level of protection and that the Town Council holds all the required licences for software.

Personnel security

The Town Council will screen new employees, contractors or anyone else who will have access to information assets. This includes checking references, gaps in career history, confirmation of academic and other qualifications and an independent check of identity by passport or other official documentation.

The Town Council has a disciplinary policy that can be used in the event that there is a breach in security controls.

The Clerk will receive training to ensure that the Clerk understands and is able to apply the security policy.

Physical and environmental security

The Council's computer information is stored on an independent system.

All paper records are stored in locked filing systems, cupboards or archive rooms at the Town Council offices. The office is locked when not in use and is not left unattended.

The Town Council computer systems are password protected and protected by fire walls and anti-virus software. The backup drive is password protected.

The Town Council does hold information as defined by the Data Protection Act/General Data Protection Act as sensitive personal data but it is limited to employees.

There is no public access to the information systems. Requests for information received under the Freedom of Information Act and the Data Protection Act will be dealt with in accordance with the relevant legislation.

This policy will be reviewed every two years or more frequently where new regulations necessitate a review

This policy should be read in conjunction with:

- Data Protection Policy
- Information Security Asset Inventory
- Stotfold Town Council Privacy Notice
- Document Retention Policy