Information Security Policy

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 for information 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

Security policy

Information Security is very important to Stanwick Parish Council.

The Parish Clerk will be expected to undertake training on information security as appropriate from suitable sources such as Northamptonshire CALC, Society of Local Council Clerks and the IT officers at East Northamptonshire Council.

The Parish Council will ensure that elementary precautions concerning computer security etc are in place to protect the Councils computers.

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

Parish Council computer records will be regularly backed up on to an independent drive and stored separately from other computer records.

All security problems will be reported to the Parish Council and minuted accordingly. In the event of a serious incident the council chairman will be notified immediately.

The Parish Council has a Data Protection Policy.

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

Organisational security

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

Where appropriate the Parish Council will seek external expert advice.

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

Asset classification and control

The Parish 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 Parish Council holds all the required licenses for software.

Personnel security

The Parish 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 Parish Council will insist on confidentiality agreements for people who are given access to sensitive information assets.

The Parish 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.

The Clerk will be made aware of the reporting procedure for all security problems.

Physical and environmental security

As the Clerk is expected to work from home there are specific security issues. The Council's computer information is stored on an independent system. All paper records are stored in dedicated filing systems.

The Parish Council computer systems are password protected and protected by fire walls and anti- virus software.

The Parish Council does not hold any information as defined by the Data Protections Act's eight categories of sensitive personal data.

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.