PRESTEIGNE AND NORTON TOWN COUNCIL

DATA & IT SECURITY POLICY

The Data Protection Act says security should be appropriate to:

- the nature of the information in question; and
- the harm that might result from its improper use, or from its accidental loss or destruction.

The Act does not define "appropriate". But it does say that an assessment of the appropriate security measures in a particular case should consider technological developments and the costs involved. The Act does not require an organisation to have state-of-the-art security technology to protect the personal data it holds, but a review of your security arrangements should regularly occur as technology advances. There is no "one size fits all" solution to information security, and the level of security chosen should depend on the risks to the organisation.

For computer security:

- Firewall and virus-checking installed on computer.
- Operating system set up to receive automatic updates.
- Download the latest patches or security updates, which should cover vulnerabilities to computer automatically
- Only allow Members access to the information they need to carry out their work and do not share passwords.
- Regular back-ups of the information on your computer system taken and kept in a separate place.
- All personal information will be removed before disposing of old computers (by using technology or destroying the hard disk).
- Anti-spyware tool installed. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

For using emails securely:

- Before sending consider whether the content of the email should be encrypted or password protected.
- Take care when typing in the name of the recipient; some email software will suggest similar addresses that have been used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave"

- the auto-complete function may bring up several "Daves". Make sure to choose the right address before clicking send.

- To send an email to a recipient without revealing their address to other recipients, make sure blind carbon copy (bcc) is used , not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Take care when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- To send a sensitive email from a secure server to an insecure recipient, security will be threatened. Check that the recipient's arrangements are secure enough before sending your message.

For using faxes securely: NOT USED

For other security:

- Confidential paper waste will be shredded/burnt
- Physical security of premises considered

Training of staff:

- to know what is expected of them;
- to be wary of people who may try to trick them into giving out personal details;
- to use a strong password -
- to not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- to not to believe emails that appear to come from the bank that ask for account, credit card details or password (a bank would never ask for this information in this way);
- to not open spam – not even to unsubscribe or ask for no more mailings. Delete the email and use spam filters on the computer.

Agreed 11th June, 2013.
Reviewed Annually.
Last Review May 2018