NEW RADNOR COMMUNITY COUNCIL

DATA PROTECTION AND SECURITY POLICY

In preparation for the GDPR (General Data Protection Regulation) in May 2018 the Community Council has produced the following additional documents –

- *Data Audit Schedule*
- *Information and Data Security Policy*
- *Email and general contact privacy notices*
- *GDPR Consent to hold contact information form*
- *Document Retention and Disposal Policy with Appendix.*

Personal Data stored will be emails, names, addresses and telephone numbers as supplied by the data subject during routine contact with the Council and from those making contact through the website. It will be stored as detailed below.

Information stored will not be released to any other organisation or person outside the Community Council without the express permission of the data subject.

Details of the data stored will be available free of charge on request and the Council undertakes to supply this within the statutory time limit current at the time of the request.

The Council will take all possible precautions to protect personal data and details of the security arrangements are below.

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.

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 you have 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 you choose the right address before you click send.
- To send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), 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.

Created November, 2017.
Last Reviewed May 2018.