Shimpling Parish Council

RISK ASSESSMENT				
Parish Council Email Addresses				
POTENTIAL HAZARDS	**Low**	**Medium**	**Medium to High**	**High**
1. Increase in data breaches	**X**			
2. Use of Unauthorised IT Equipment	**X**			

SITUATION

The National Association of Local Councils (NALC) has identified that the number of Phishing and Spam emails has grown significantly. This inappropriate Cyber activity poses a growing threat to the security of Parish Council (PC) data and "is seen as the top root cause of all data breaches". This has driven a review of the email infrastructure used by the PC to ensure its appropriateness.

ANALYSIS

The current email standard for the PC is for each person on the council to have a .gov.uk account which provides an email address in the form xx.shimpling-pc@gov.uk, where xx is the individual's initials. These email addresses are intended for PC business only, although there is currently no mechanism to enforce this.

On reviewing 20+ Parish Council's, primarily across Suffolk and East Anglia, it was obvious that no standard approach to the use of email systems is in place. The four (4) main options used, listed in their order of (security) effectiveness, are:

1. Personal email address
2. Defined email address, provided on a generally available external system
3. Defined email, provided by a service based external system (where you pay for email system)
4. Organisation email, provided by own email system

Whilst options 1 & 2 are effectively free, options 3 & 4 have significant costs associated with them. Option 4 is considerably more expensive than option 3 and is only really appropriate for larger organisations.

The majority of the data which the PC has access to and uses is also generally available in the public domain, as shown in the Shimpling Personal Data Audit Questionnaire (SPDAQ). There is a small amount of communication which comes in from associate organisations and the public containing data potentially needing to be kept secure, most notably personal data but also some which may be organisation sensitive.

The current option being used by the PC meets the requirements set out in the Data Protection & Information Management Policy, specifically section 13.4, and the Privacy Notice.

ACTIONS

- Monitor data breaches as a result of email security issues (SPDAQ Part E)
- Monitor the use of BYOD (DP&IMP Section 19) for compliance