Ottery St Mary Town Council

IT Security Policy

Adopted April 2018

Review Date: April 2020

The Policy

This policy has been drawn up taking into account the extent of current IT systems and usage, standard technology and cost. The measures are intended to be appropriate for the harm that could result from security breaches and the nature of the information and data processed.

Policy review

This policy will be reviewed annually and whenever there are significant changes to IT systems and usage.

Management

Overall management of the Council's IT systems is the responsibility of the Town Clerk, but all users also have a duty to maintain the security of the Council's IT systems and the data held on them.

Breaches of this policy will be considered a disciplinary matter.

Passwords

All computers and laptops must be password protected using suitably strong passwords consisting of a mixture of letters and numbers or symbols. Passwords must be changed every 90 days or when there is a change in staff or if there is a chance that they may have been compromised.

Password Construct Guidelines

Unless stated otherwise in this policy, all passwords must be strong passwords. Strong passwords have the following characteristics:

- At least 8 characters long
- A mix of alphabetic, numeric and special characters
- Not a word in any language (including names, familiar terms and slang)
- Not based on personal information and do not have an association with the system or facility being accessed

- Not a pattern – e.g. ‘456787654
- Not any of the prohibited formats read backwards
- Are not any of the prohibited formats prefixed / suffixed or with the addition of 1 or 2 characters
- Are not passwords used for access to personal facilities inside or outside of work. One way of constructing a strong password is to find a phrase that you will readily remember and take initial letters and numbers from that phrase for your password. So for example, ‘We like to go away two times per year’ could become ‘Wl2ga2tpy’ Please do not use this particular example. You may use the same strong password for access to more than one Council system or facility.

Good practice

Use different passwords for each system, programme or website that is accessed. Passwords should not be written down anywhere that they can be easily found by an intruder.

Software

Security updates for software that fix any vulnerability that has been discovered will be downloaded automatically.

Laptops and portable media

Laptops and portable media (such as memory sticks, disks or so on) that are taken out of the office should be transported securely and protected with encryption software.

Good practice

Consider whether it is appropriate to take sensitive or personal data out of the office. How sensitive is the information? Could it cause damage or distress to the people concerned? Highly sensitive data should not be taken out of the office.

Keep laptops and portable media out of sight, e.g. not left on view in an unattended car.

Disposal of equipment

When disposing of equipment information should be securely deleted.

Good practice

Information can be recovered even if someone thinks they ‘deleted’ it using the delete button. Securely deleting information will mean using techniques like overwriting the material a number of times or, if you are getting rid of the equipment, destroying the hard disk.

Back ups

Weekly back-ups are taken on an external hard drive which is held in the office safe.

Good practice

A monthly test of recovering information from the back-ups should be made to ensure that all files have been correctly backed up.

Internet and email

Firewall and virus protection is maintained on all computer systems and kept up to date. The current programme is ESET Smart Security.

Good practice

Take care to avoid downloading potentially dangerous files or software. The following can help:

- Do not attempt to open any suspicious e-mails or attachments. Treat as suspicious e-mails from:
  - Anonymous senders
  - Strangers addressing you in a familiar manner
  - Non-standard addresses
  - Banks or other institutions asking you to confirm your account information.
  - Look out for inconsistencies in the sender's email address and any links to webpages – for example, a domain name such as businesslink.co.uk rather than the correct businesslink.gov.uk.
  - Be especially wary of any of the above that contain attachments with .EXE, .SCR or VBS file extension names.
  - Malicious programmes can also lurk in more familiar forms; even Microsoft Word and Excel attachments can contain macro viruses.
  - Never forward virus warning messages to everyone on an e-mail list or contact group. This can spread just as fast and cause as many problems as a virus.
  - Never forward funny or joke programmes to others. If you must pass information, send them a URL link and not the programme file itself.
  - If you are in any doubt, save suspicious attachments to your local directory, then use virus defence software to examine it in more detail
  - A simple check is to telephone the alleged sender (if possible) to confirm their identification

Junk email

Unwanted email, sometimes known as junk or spam email, is unsolicited email advertising. Unwanted email clogs up your inbox and the internet. It can also carry viruses and spyware.

Good practice

Microsoft Outlook has a junk email filter but some unwanted emails inevitably get through. The filter is set to “low” which removes most obvious spam to a junk mail folder which should be checked daily to make sure that no genuine messages have been caught. It is also possible to block persistent offenders.

Training

Staff will be provided with training and updates on IT security risks as required.