Shavington-cum-Gresty Parish Council
159 Main Rd, Shavington, Crewe, CW2 5DP

Use of personally owned computer equipment for council business

Approved 1 December 2021

Members who opt to use their own computers and tablets must undertake to maintain an appropriate level of security on devices used for accessing Council information. The ICO has stated 'Permitting a range of devices to process personal data held by an organisation gives rise to a number of questions a data controller must answer in order to continue to comply with its data protection obligations. It is important to remember that the data controller must remain in control of the personal data for which he is responsible, regardless of the ownership of the device used to carry out the processing.'

Detailed guidance is provided below but in brief security arrangement required would include:

- Maintaining an up to date antivirus solution.
- Applying system and software patches and updates as and when they are released.
- Enabling personal firewalls.
- Maintaining password or other access controls (such as personal identification numbers, or PINs) on devices and accounts.
- Storing documents, emails or other files containing information related to the business of the Council in places where others who are not entitled to the information cannot gain access to them. This applies, for example, when storing documents on a shared computer, and rules out using a joint email account.

Securing personally owned computer equipment

General.
Where a member is using privately owned equipment for processing personal data the following guidance should be followed as a minimum:

- Passwords and PINs to lock the device or screen when it is not in use should always be used.

- Different passwords for Council and personal business should always be used. Passwords for council systems should never be shared; not even with ICT staff.

- Passwords should be at least 8 characters in length and contain a mix of upper and lower case letters, numbers and special characters and should not contain common words, family names or part of your user name. Using phrases that are easy to remember are better than single words however long; for example "Mysmalldog1#".

- If other people have access to the computer you use for your council business (e.g. a family or business computer) there must be separate accounts on the computer for each person and you should log off every time you have finished using it.

- If you lose, or suspect you have lost, Personal information relating to an individual regardless of how it happened e.g. laptop stolen, computer virus you should assess the seriousness of the information getting into the wrong hands and take the following actions:

    - If you have had computer equipment stolen, whether that be personal or council owned, you must report it to the police and obtain a crime report number. This will be required in any insurance claim.
    - If you have lost any council owned equipment you must report it to the clerk who will then discuss with the Data Protection Officer whether the incident warrants reporting to the Information Commissioners Office.

Personal computers and laptops.
If you are using a personal computer or laptop you should:

- Always have an up-to-date antivirus solution in place. This will always mean having a personal firewall configured on your computer, and will involve either having appropriate anti-virus software installed, or keeping built-in antivirus protection updated. Most commercially available products such as Norton, Kaspersky, McAfee etc provide both levels of protection. They may also have other features such as internet browsing protection, parental controls etc. There are free antivirus products available but the old adage “you get what you pay for” in the internet security world applies.

- Any antivirus product should be configured to automatically scan your computer regularly (weekly) and should also be configured to automatically download and apply the latest updates.

- You should always load security updates provided for the applications on your computer when prompted.

Tablets and smartphones

- There are antivirus products (apps) available for mobile devices (tablets and smartphones) but as they operate in different ways from computers and laptops generally the security of such devices can be managed through the device settings. Apple and Android devices may still be subjected to vulnerabilities though these are usually introduced through cheap or free apps from illicit download sites. The use of an internet security app (such as Webroot) which helps to secure web browsing activities is suggested where appropriate. The biggest risk to information on mobile devices is when the device is lost or stolen. Having said that there are a number of points that should be considered when using mobile devices:
    - Always run security and operating system updates when prompted.
    - Maximise access security for instance by having a 4 digit access pin and finger print recognition
    - Do not try to bypass the settings in the device (known as jailbreaking).
    - Only use apps from reputable sources such as the Apple App Store, Google play store or similar (e.g. Amazon). It is recommended to use apps only from the appropriate Store for the device.

Email security
Members who process emails related to council business that may contain personal information about employees, other members or citizens should ideally do so in their allocated council email account. This

removes many of the compliance requirements from the individual member. The following guidance should be followed:

- Routinely auto forwarding email from one account to another, such as from a Council email address to a private address presents a risk to the council as there is no control regarding what information is being forwarded. The Council has to ensure that personal data being sent from its own system is adequately protected.

- Keep an email account for Council matters that is separate from work or business, private and family matters. Although this may seem onerous the risk of information leakage is greater when all email is held in one account.

- Have separate passwords for each email account.

- Beware of using “reply to all”, forwarding emails, using the carbon copy (cc) function and distribution lists when forwarding personal data as you must ensure everyone you are sending it to is entitled to receive it.

- Never click links in emails except when you are expecting the email and you recognise the sender (such as when you are expecting a password reset or account activation).

- Be wary of opening attachments you are not expecting.

- Beware of rogue emails trying to gain your personal information (known as Phishing). Some of these emails appear very genuine.

- Many email providers are using web versions of their software for example Hotmail, AOL, Gmail. Many of these are hosted outside the EEA and may not comply with the Data Protection Act. If you are unsure as to where your information is being stored you as a data controller should contact your provider and seek a written assurance regarding where you data is being held.

- Never let other people routinely deal with your Council email on your behalf; they may not be entitled to view the contents.

File security

Documents which contain personal information such as letters from residents or print outs of information should be secured so that they cannot be accessed by people not entitled to see them. This applies whether the document is in paper or digital format. When dealing with information the following guidance should be followed:

- Personal data and personal sensitive data related to residents, employees of the Council, or other Members should never be held in an account or storage area that can be accessed by other people.

- Keep separate file structures for council and non-council business.

- Consider password protecting documents.

- If you are storing documents containing personal and personal sensitive data on the hard drive of a computer you should be aware those documents exist even after you have deleted them or formatted

Shavington-cum-Gresty Parish Council
159 Main Rd, Shavington, Crewe, CW2 5DP

the disk so when the computer is no longer required you should ensure the hard drive is physically destroyed.

- If you use a cloud based storage system such as Dropbox, Apple's iCloud, Google Drive, Microsoft One Drive then you need to satisfy yourself that the storage of personal information is compliant.

- Be wary of transferring personal information via USB stick. Apart from the risk of transferring viruses and other malware, they are easy to mislay. If you must use a USB stick to transfer personal information ensure it is of the encrypted type or that the files on the stick are either encrypted or password protected. Do not allow others to use the same stick.

Wireless hot spots

The increasing coverage of free public wireless networks means devices can frequently be connected to the internet from many public spaces such as hotels, restaurants airports. However, there are a number of security concerns related to their use:

- You can never be sure if the wireless access point you are connecting to is actually what you think it is, for example anyone with a mobile phone or computer can set up a wireless hotspot in a coffee shop and call it "cafe secure Wi-Fi".

- You cannot be sure who else is connected to the same network, and whether they can capture your data.

- There are a number of things you can do to reduce the risk when using open Wi-Fi connections:
    - If there are secure connections available choose one of these instead.
    - Turn of data sharing application and location aware services. Turn on Wi-Fi only when you need it.
    - Avoid using other websites that require you to input a user name and password such as online shopping and banking when connected to an open connection.

This is to certify that I wish to use my own personal ICT equipment for the processing of council information. I have read and understood the ICT guidance for members above and will ensure adequate technical and physical security measures in place to protect the information related to the business of the council. I understand that I may from time to time be asked to provide evidence that appropriate security measures are in place.

Name…….

Sign……

Date……

This form is to be signed annually and to be returned to the clerk once completed.