Acton Burnell, Frodesley, Pitchford, Ruckley and Langley Parish Council

INFORMATION TECHNOLOGY POLICY

Contents

Acton Burnell, Frodesley, Pitchford, Ruckley and Langley Parish Council

INFORMATION TECHNOLOGY POLICY

Statement of purpose

The purpose of this policy is to ensure that all employees and any volunteers or Councillors using ABFPR&L PC information technology have a clear understanding of what is and is not permitted. This will ensure the appropriate use of the council's equipment, safeguard the security of its IT systems and data and assist compliance with Data Protection law. The policy should be read in conjunction with our Personal Data Management and Audit Policy.

Policy coverage

This policy covers the security and use of all the Council's information and technology equipment such as laptops and tablets and personal devices which are used to access Council information. It also includes the use of email, internet, cloud storage and the Council's website. This policy applies to Council employees, Members, contractors, volunteers and other members of the public when using Council equipment and software. The policy applies to all information, in whatever form, relating to the Council's activities, and to all information handled by the Council relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by the Council or on its behalf.

Training

All staff should be made aware of data protection and information security requirements at their induction. Any employee, volunteer or Councillor undertaking work for the Council may request training to support their knowledge and use of required technology or understanding or information security and data protection. Requests should be made in writing to the Clerk or Chairman of the Council.

Passwords

All Council devices must be password protected. Passwords should be "strong" and use uppercase and lowercase letters, numbers and a special character. The Clerk may share passwords with Members of the Council, on request, in order that they may access the Council's systems in the event of a period of leave, contract termination, or if the Council is investigating the Clerk's use of equipment under this policy.

Passwords for websites and apps, in particular Internet banking passwords, should not be saved to any device. Passwords should not be reused and each device, website or app should have a unique password.

Acceptable usage of council technology

Individuals are accountable for all actions on the IT systems. Individuals must not:

- Leave their user accounts logged in at an unattended and unlocked computer
- Attempt to access data that they are not authorised to use

- Give or transfer council data or software to any person or organisation outside the council without the appropriate authority to do so
- Download software onto Council devices without ensuring that it is legitimate and secure
- Store personal files, such as music, video, photographs or games on council IT equipment
- View personal or confidential information on their device where it may be overlooked by members of the public

Internet and email conditions of use

The council's internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the council in any way, not in breach of any terms and conditions of employment and does not place the individual or the council in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Internet Access Unacceptable Behaviour

In particular, the following is deemed unacceptable use or behaviour:

- Visiting sites that contain obscene, hateful, pornographic or illegal material
- Perpetrating any form of fraud, or software, film or music piracy
- Using the internet to send offensive or harassing material to other users
- Downloading commercial software or any copyrighted materials belonging to third parties, unless the download is covered or permitted under a commercial agreement or other such licence
- Hacking into unauthorised system, sites or files
- Publishing defamatory and/or knowingly false information about the council, colleagues, Members and/or customers on social networking sites, blogs, wikis, or any online publishing format
- Revealing confidential information about the council in a personal online posting, upload or transmission; including financial information and information relating to customers, business plans, policies, employees, Members and/or internal discussions
- Undertaking deliberate activities that waste council effort or networked resources
- Introducing any form of malicious software into the council's technology systems

Email Usage Unacceptable Behaviour

In particular, the following is deemed unacceptable use or behaviour:

- Distributing, disseminating or storing images, text or materials that are illegal, or might be considered indecent, pornographic or obscene

- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered harassment
- Use of council communications systems to set up personal businesses or send chain letters
- Forwarding council confidential messages to external locations
- Accessing copyright information in a way that violates the copyright
- Unauthorised use of a password or mailbox
- Broadcasting unsolicited personal views on social, political, religious or other non-council related matters
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste council effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

Council officers and members should regularly delete or archive emails when they are no longer current or required in order to restrict the size of their mailboxes and reduce the risk of incoming emails being rejected. Emails should not be kept longer than they are required in line with our Personal Data Management and Audit Policy. Individuals should be aware of the characteristics of spam and phishing emails and should not reply to these emails, but add the sender to their email system's Blocked Senders List.

Any use of text messaging for council purposes follows the same acceptable use guidelines as emailing above. Before using text messaging, individuals should consider whether this is an appropriate or professional method for the required communication.

Viruses

All PCs must have antivirus software installed to automatically detect and remove viruses. Individuals must not remove or disable antivirus software.

Actions upon Termination of Contract

All council equipment and data, for example laptops and mobile devices, must be returned to the council at termination of contract. All council data or intellectual property developed or gained during the period of employment remains the property of the council and must not be retained beyond termination or reused for any other purpose. Users must delete all council information from any personal device upon termination of their employment, or if the device is repaired, exchanged, sold, given away or otherwise disposed of. Users may be required to provide a written undertaking that this will be done.

Use of personal devices for council work

Upon request, the council will consider providing council owned mobile devices or computer equipment for employees or Councillors. As the council does not currently supply mobile phones

and computer equipment to all employees and Councillors, the council accepts that personal devices will be used to access and store council information.

The policy applies to use of personal devices for business purposes at all times, both during and outside office hours and whether or not users are at their normal place of work.

This policy recognises that personally-owned mobile devices are and will be used to access council information. The use of any personal device to process and access council information creates risks including those relating to data protection, virus infection, copyright infringement, unintentional or unlawful compromise of data and even loss or theft of device and/or data. The council, its officers, Members and volunteers, are committed to processing all personal data in accordance with current UK Data Protection law, as specified within the council's Personal Data Management and Audit Policy, regardless of the device used to access the information. Users are required to keep council information and personal data secure. This applies equally to council information held on council systems and devices, or accessed/held on personally-owned devices.

The council is the owner of all council information and the contents of council systems together with everything which is created on, transmitted to, received on or printed from, or stored or recorded on any device, in each case during the course of the council's business or otherwise on the council's behalf, irrespective of who owns that device. The council reserves the right to request access to inspect, or delete council information held on a personally-owned device to the extent permitted by law and for legitimate business purposes. Every effort will be made to ensure that the council does not access the private information of the individual.

User responsibilities

Users are responsible for:

- The security of council information and of the device on which the information is held
- Storing council information on the personal device only for so long as necessary
- Deleting council information from the personal device when no longer required, or sooner if required by the council to delete it
- Ensuring where possible that the device has an up to date operating system and antivirus protection
- Complying with this policy and the related policies

Data access and storage

Use of any personal device for council purposes is at the user's risk and the council is not liable for any losses, damages, or liability arising out of such use, including but not limited to loss, corruption or misuse of any content or loss of access to or misuse of such personally-owned device, its software or its functionality. Storage using personal devices can put confidential information at risk of

compromise and may be subject to varied technical standards and support, as well as access by third parties.

Confidential or sensitive information should be stored on and accessed from council information systems and council managed storage to ensure security of and appropriate secure access to the information. Users should only store the minimum amount of information necessary to carry out the required task on a personal device. A temporary cache may be held on the device, therefore any confidential, sensitive or personal information should be deleted from the device as soon as the information is no longer required.

Costs associated with mobile devices

The Council will provide the Clerk with a contract mobile SIM card to cover the costs of telephone usage related to their job. This is provided for business use only and the Clerk will not use this SIM card to make personal calls. The Clerk will take care not to incur any additional costs not included in the contract, such as data roaming. The use of mobile devices overseas can lead to potentially significant costs, for example through data roaming, as well as risks to the device. Users must obtain approval for overseas travel with a council-issued mobile SIM card. There is currently no policy on the reimbursement of costs or data plans for personal devices.

Device and Physical Security

Information should be protected against loss or compromise when working remotely, for example at home or in public places. Devices accessing council information must have a strong password, passcode or PIN enabled to reduce opportunity for unauthorised access. These must be kept secure. The device should be set to automatically lock if inactive for 5 minutes or less, or locked manually using Ctrl, Alt and Delete keys. Devices used to access and or store confidential, personal or sensitive data should be subject to additional protection measures (such as encryption) to reduce opportunities for loss or compromise of the information. Devices should, where possible, have operating system and antivirus updates enabled. When unattended, the device must be locked (password, passcode or PIN protected).

Users must take responsibility for a device and not leave it unattended in busy public areas, public transport or in a car. Laptops must be carried as hand luggage when travelling.

Devices that are the property of the council must be returned upon change of user or termination of employment. They must not be sold, given away or otherwise disposed of by the user. If devices are not returned (after a reminder process) the matter will be treated as a disciplinary matter. The matter may also be passed to the Police for consideration of further action or for recovery via civil litigation.

Acton Burnell, Frodesley, Pitchford, Ruckley and Langley Parish Council

INFORMATION TECHNOLOGY POLICY

Reporting loss or theft

In the event of loss or theft of any device containing Council information, irrespective of whether it is council-issued or personally-owned, the user must act promptly to minimise the risk of compromise to council information by immediately:

- Changing any passwords that may have been used on the device, e.g. banking
- Reporting theft of device to the Police
- Reporting loss or theft of mobile phone to the mobile network carrier directly
- Reporting any specific known data protection breaches in line with procedures outlined in our Personal Data Management and Audit Policy.

Data backup systems

The Council's data held on the Clerk's laptop should be backed up fortnightly to a removable hard storage drive and the council's Microsoft 365 cloud storage account to insure data is protected against loss.

The data stored on removable media is the responsibility of the individual who operates the devices. The removable device must not be used to keep data that is not backed up securely in a central location. Removable media should be physically protected against loss, damage, abuse or misuse when in use, storage and transit. All data should be removed from the removable drive once it is no longer in use.

External contractors

Where external contractors are used to provide technology, such as the Council's website, email or cloud storage systems, the clerk should ensure that the contractors have the required data protection, backup, and information security policies and procedures in place to protect the Council's data and systems from security breaches.

Council-owned information held on third-party websites

If you produce, collect and/or process council-related information in the course of your work, the information remains the property of ABFPR&L Parish Council. This includes such information stored on third party web sites such as webmail service providers and social networking sites, such as Facebook.

Monitoring and breaches of this policy

All data that is created and stored on council computers is the property of the council. The council currently does not monitor emails or internet usage. However, investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy, for example:

- complaints are received about malicious emails
- evidence of criminal activity or sending/downloading pornographic images

- staff are spending unreasonable amounts of time visiting non-work related internet sites or sending personal emails

The council has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure system security and effective operation, and to protect against misuse. The council maintains the right to examine any systems and inspect any data recorded in those systems, which includes but is not limited to internet access and email or messaging content. As a matter of compliance with this policy and meeting the regulatory requirements asked of the council, the council reserves the right to use monitoring software in order to check upon the use and content of emails. The council maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use. Before monitoring is undertaken, all staff would be informed and provided with information on the council's approach to monitoring. Any monitoring will be carried out in accordance with audited, controlled internal processes, current UK Data Protection law, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000. Any information obtained from monitoring would only be used for the purpose it was obtained.

Any individuals who suspect a breach of security policy must report it without delay to the Clerk or Chairman of the Council. All breaches of information security policy will be investigated and where investigations reveal misconduct, disciplinary action may follow in line with the council's Staff Disciplinary Policy and procedures. Breaches of the IT Policy by Members could contravene the Code of Conduct and action may result from this contravention.

Policy monitoring and review

This policy will be reviewed annually at a full Council meeting. The Clerk is responsible for monitoring the use and security of the Council's technology on an ongoing meeting. The Staff Appraisal Committee is responsible for assessing the Clerk's use and understanding of technology security at the Clerk's annual appraisal.

Date Adopted:	8/3/22	
Date Reviewed:	3 May 2023	
Date of Next Review:	September 2024	