BLEAN PARISH COUNCIL

Information Technology Policy

Purpose

Blean Parish Council is committed to establishing clear parameters for how Councillors and staff use Council-provided technology or equipment in the course of their duties.

This helps to:

• Set clear expectations for appropriate use of equipment and systems.

• Raise awareness of risks associated with IT use.

• Safeguard the council's data and digital assets.

• Clarify what constitutes acceptable and unacceptable use.

• Outline the consequences of policy breaches. The Parish Council's equipment is not for personal use at any time and remains the property of Blean Parish Council.

Monitoring

As an IT provider, the Parish Council has a right to monitor the use of its IT equipment and systems, if it has a legitimate reason for doing so. Councillors and employees are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant Data Protection legislation and privacy laws. Others may be included in monitoring if they access or use the Parish Councils' systems, for example a Council email address or access the wi-fi as a hirer or visitor.

Scope of this Policy

This policy applies to all Councillors and staff regardless of their working location or working pattern, including those working from home, in the office or working flexibly or part-time. It sets out the expectations for the appropriate use of IT equipment and systems provided by the Council.

Computer use

Hardware

Blean Parish Council computer equipment is provided for Parish Council purposes only. All computer and other electronic equipment supplied should be always treated with care and respect. Computer equipment is expensive and any damage sustained will have a financial impact on the Parish Council.

Computer and electronic hardware should be kept clean. Every precaution should be taken to prevent it getting damaged especially from liquids and food.

Equipment

Councillors and staff are not to purchase any computer or mobile device equipment including software unless authorised by the Parish Council.

Personal disks, USB stick, CD's, DVD's and data storage devices cannot be used on the Parish Councils systems without prior approval of the Parish Clerk. Using a portable device to make a personal Wi-Fi hotspot, bypassing existing Wi-Fi, is prohibited. Any faults, damage or repairs must be reported to the Parish Clerk who will report to the Parish Council.

Portable equipment
Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capabilities and access to the internet. All portable equipment must be stored safely and securely when not in use in the office. This includes when travelling between working locations or working from home. Portable equipment (unless locked in a secure cabinet or office) should be always kept with or near the user. It should not be left unattended at any time when away from Parish Council premises, including in parked vehicles or at any Council or non-Council premises. If an item of portable equipment is lost or damaged this should be reported immediately to the Parish Clerk, and then to the Council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the full cost of the repair or replacement. To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken in the Parish Office without the prior written permission of the Council. This includes mobile telephones with a camera function, camcorder tape or other recording device for sound or pictures – moving or still. Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

In addition, the Parish Council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for Council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sort from the Parish Clerk.
If webcams are used in the Parish Office care should be taken to ensure that any sensitive information or details are not able to be seen in the background of any camera. Best practice is to have a plain wall behind you during the call.

Use of Own Devices
Personal laptops and other computers or other devices should not be bought into work and used to access the Parish Council IT systems during working hours, unless this has been authorised by the Parish Clerk. This is to ensure that no viruses enter the system, to prevent time being wasted during working hours on personal use and to assist in maintaining security, confidentiality and data protection. For continuity purposes, calls made to external parties must be made on the Parish Council landlines or mobile phone to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any emails sent from own devices should be sent from a Parish Council email account and should not identify the individual's personal email address. Councillors and staff that use the Council systems, are expected to use all devices in an ethical and respectful manner, and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the Council carries a high degree of risk. For staff, may result in disciplinary action, including summary dismissal (without notice). In the case of legal proceedings, the Parish Council may need to temporarily take possession of a Council owned device to retrieve the relevant data. Councillors and staff to use their own devices via the Parish Council's infrastructure must ensure that they:
• Use either a 6-digit pin, password or fingerprint to protect their devices from being accessed. For smartphones and tablets this should lock the device after 3 failed login attempts.
• Always password protect any documents containing confidential information that are sent as attachments to an email and notify the password separately
• Ensure secure Wi-Fi networks are used.

• Ensure that work related data cannot be viewed or retrieved by family or friends who may use the device.
• Inform the Parish Clerk immediately if their devices are lost, stolen or inappropriately accessed where there is a risk of access to Council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

Personal data relating to the Parish Council should not be saved to any personal accounts with third party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits Councillors and staff to remain logged in between sessions. Personal information and sensitive data should never be saved on Councillors, or staff's own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time. If removable media are used to transfer data (e.g. USB drivers or CDs), the user must also securely delete the data on the media once the transfer is complete.
Councillors and staff who open any attachments should ensure that any cached copies are deleted immediately after use. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.
Any work done on user's own equipment should be stored securely and password protected. Prior to the disposal, any Parish Council owned device that has work data stored on it, and in the event of a user leaving the Council, the Parish Clerk should access the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device. Councillors and staff must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing Council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss because of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable.

Health and Safety
Staff who work in Parish Council offices will be provided with an appropriate workstation. The Parish Council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. All user accounts must be protected by strong, secure passwords. The Council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

Access to Passwords
• Passwords are personal and must not be shared under any circumstances.
• Only the assigned user of an account may access or use the associated password.
• Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Parish Clerk, in a secure file stored on the Parish Council's cloud storage, only to be accessed in an emergency. Passwords should not be stored in plain text or written down. Immediately change password if compromise is suspected.
Responsibility •
Users are responsible for creating and maintaining secure passwords for their accounts.
The IT security provider and Parish Clerk is responsible for:

• Managing system/service credentials.
• Enforcing passwords polices.

Monitoring

The Parish Council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. The Parish Council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers.

Regulations 2018.

Monitoring of an employee's email will be conducted in accordance with an impact assessment that the Parish Council will carry out, to ensure that monitoring is necessary and proportionate. The information obtained through monitoring may be shared internally, including with relevant Councillors and IT staff if access to the data is necessary for the performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place. The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted. Councillors and staff have several rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the Parish Council's data protection policy. Such monitoring and the retrieval of the content of and messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation. The Parish Council reserves the right to inspect all files stored on its computer systems to assure compliance with this policy. Any use that the Parish Council considers to be 'improper', in terms of the content, may result in disciplinary proceedings.

Remote working

Increased IT security measures apply to those staff who work away from their normal place of work (e.g. working from home or any other different venue), as follows:

• The location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc:
• Any data printed should be collected and stored securely:
• All electronic files should be password protected and the data saved to the council's system/services when accessible:
• Papers, files or computer equipment must not be left unattended at any premises unless arrangements have been made with a responsible person at a premise for them to be kept in a locked room or cabinet if they are to be left unattended at any time:
• Any data should be kept safely and should only be disposed of securely:
• Papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed:

Email

Parish Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Parish Councillors and staff need to be careful not to introduce viruses onto Council systems and should take proper account of the security advice below. On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors and staff users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively. These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, Councillors and staff should ask the Parish Clerk rather than assuming they know the right answer. All Councillors and staff who need to use email as part of their role will be given their own Council email address and account. The Council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

Use of the Internet

Copyright

Much of what appears on the internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the Council and damages being awarded. Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying. Copyright and database law can be complicated. Councillors and staff should check with the clerk if unsure about anything.

Trademarks, links and data protection

The Council does not permit the registration of any new domain names or trademarks relating to the Parish Council's names or products anywhere in the world, unless authorised to do so.

Accuracy of information

One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraires. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

Use of social media

Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

Personal use of social networking/media and chat sites are not permitted during working hours, unless accessing the Parish Council Social media pages in line with work.

The Parish Council recognises the importance of Councillors and staff, joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable. However, inappropriate comments and postings can adversely affect the reputation of the Council, even if it is not directly referenced. If comments or

photographs could reasonably be interpreted as being associated with the Council, or if remarks about it could be regarded as abusive, humiliating, sexual harassment or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors and staff should be aware that parishioners or other local organisations may read Councillors and staff personal comments and posts, to acquire information. Therefore, even if the council is not named, care should be taken with any views expressed. Councillors should always be mindful of the Members code of conduct and Nolan Principles. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the Council.
Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air Council concerns or complaints: these should be raised with the Council or formally through the grievance procedure.

Misuse
Misuse of IT systems and equipment that is not in line with the Council's standards of conduct will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings.