Buckland Parish Council
Information Technology (IT) Policy

Digital Communication

Buckland Parish Council ("Council") promotes the use of internet and electronic mail to improve the efficiency and effectiveness of Council's functions. However, these facilities must be used responsibly and lawfully.

Communications from Council will meet the following criteria:

(i) Be civil, tasteful and relevant;

(ii) Not contain content that is knowingly unlawful, libelous, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive;

(iii) Not contain content knowingly copied from elsewhere, for which Council does not own the copyright;

(iv) Not contain any personal information – i.e. names, addresses, email addresses, IP addresses and cookie identifiers;

(v) Email communications shall include the standard Council disclaimer.

Use of Email

The following procedures are intended to ensure a complete and proper record is kept of all Council correspondence:

(i) The generic email account for the parish council and individual accounts for serving parish councillors will reside on the parish council owned bucklandsurrey.org.uk domain;

(ii) The Clerk will arrange for parish council designated email accounts to be opened for newly appointed parish councillors and ensure accounts are deleted when individuals cease to hold the position of parish councillor;

(iii) The use of email to exchange correspondence requires the same professional standards as other forms of communication – be aware that agreements made by email may have the same status as letters or formal contracts;

(iv) Councillors must use their formal parish council designated email address for council business;

(v) The Clerk is responsible for dealing with emails received and passing on any relevant mail to members or external agencies for information and/or action;

(vi) All communications on behalf of the Council will usually come from the Clerk and any other correspondence should always be copied to the Clerk;

(vii) Any correspondence from a new email address that requires data to be passed on, will need to be followed up (by the Clerk) with a Data Consent Form to be completed and returned (to the Clerk) before any action is taken with that correspondence;

(viii) Councillors who choose to communicate directly with parishioners in relation to their own personal views will need to consider whether it is appropriate to copy the Clerk. Councillors should remain mindful that copying an email to the Clerk "makes it official and subject to the Freedom of Information Act" and are advised all such emails should be sent from the email address provided to each Councillor to be used for Council business;

(ix) Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Clerks may need to access emails to prepare a response to Freedom Information or subject-access requests.

(x) In order to protect from viruses, email attachments which might contain macros (word processor and spreadsheet files) or applications, should not be opened if they are from an unfamiliar sender; they should be deleted; and

(xi) Junk mail is a hazard of internet life and efforts should be made to isolate it at source; junk mail should otherwise be deleted without opening any attachments.

Data protection

(i) Sensitive personal data should not be included in the text of emails sent, nor in files attached to them, unless the files are password protected and the password is provided to the intended recipient via a separate channel. This is to ensure compliance with the Data Protection Act 1998.

(ii) Email addresses should be treated as confidential and care taken that private email addresses are not wrongly circulated. Parish Updates, issued to members of the village email group are distributed using the blind copy addressee field.

Internet

Material should not be downloaded to the Council laptop if there is any suspicion that it may contain a virus. Material from the Internet should not be used without checking whether it is restricted by copyright or licensing law.

Website

The village website is hosted by an external company on a server located in the EU (Ireland) and encrypted using AES 256bit. A backup of the village website is automatically generated on a regular basis to safeguard against failure of the hosting company. Updates to the website are published by the volunteer webmaster and the Clerk.

Council owned laptop

The Council laptop operating system is Windows 11 Pro, Council subscribes to Office 365 and updates to windows and office are automatically applied. Bitlocker has been activated to encrypt the data held locally on the hard drive and Windows Defender is active.

Information held on the Council laptop is backed up using Microsoft OneDrive (cloud storage feature of Office 365). The data held on the Council laptop is also backed up periodically, with the benefit of password protection, to a stand-alone hard drive.

Microsoft has stated its commitment to Windows 11 and Office 365 remaining GDPR compliant.

The Clerk is responsible for ensuring the Council laptop is kept clean, is not used to access offensive material and for reporting any unresolved faults to Council.

Password and account security

Councillors and Council employees should use the National Cyber Security Centre's advice for choosing a strong password. For business continuity, the login details and passwords are stored securely and can be accessed by a locum clerk in an emergency.

Text messaging

Councillors and the Clerk may use text messaging as a convenient way to communicate at times. All are reminded that this policy also applies to such messages.

Video Conferencing e.g. Skype, Zoom, GoTo

If this medium is used to communicate please note that this policy also applies.

Social media

Social media for work purposes should be used only with the express permission of Council.

Councillors are expected to abide by the Code of Conduct and the Data Protection Act in all their work on behalf of the Council

As more information becomes available at the press of a button, it is vital all information is treated sensitively and securely. Members should take care only to copy recipients on a "need to know" basis (i.e. avoid use of "reply to all") and ensure email correspondence is deleted on a timely basis.

Councillors are expected to maintain an awareness of the confidentiality of information that they have access to and not to share confidential information with anyone. Failure to properly observe confidentiality may be seen as a breach of the Council's Code of Conduct and will be dealt with through its prescribed procedures.

Section B : The Management of Transferable Data Policy

Purpose

This policy supports the controlled storage and transfer of information by Councillors and all employees, temporary staff and agents, contractors, consultants and others working on behalf of Buckland Parish Council ("Council") who have access to and use of computing equipment that is owned or leased by Council.

Information is used throughout Council and is sometimes shared with external organisations and applicants. The use of removable media may result in the loss of the ability to access information, or interference with the integrity of information, which could have a significant effect on the efficient operation of Council and may result in financial loss and an inability to provide services to the public.

It is therefore essential for the continued operation of Council that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to Council's needs.

The aims of the policy are to ensure that the use of removable storage devices is accomplished with due regard to:

(i) Enabling the correct data to be made available where it is required
(ii) Maintaining the integrity of the data
(iii) Preventing unintended consequences to the stability of Council's computer
(iv) Building confidence and trust in data that is being shared between systems
(v) Maintaining high standards of care towards data and information about individual parishioners, staff or information that is exempt from disclosure
(vi) Compliance with legislation, policies or good practice requirements

Principals

This policy sets out the principles that will be adopted by Council in order for material to be safely stored on removable media so that the risk of loss or corruption to work data is low.

Removable media includes but is not limited to: USB memory sticks, memory cards, portable memory devices, CD / DVDs, diskettes and any other device that transfers data between systems or stores electronic data separately from email or other applications.

Any person who intends to store Council data on removable media must abide by this Policy. This requirement devolves to Councillors, employees and agents of Council, who may be held personally liable for any breach of the requirements of this policy.

Failure to comply with this policy could result in disciplinary action.

Advice and Assistance

The Clerk will ensure that everyone who is authorised to access Councils information systems is aware of their obligations arising from this policy.

A competent person should be consulted over any hardware or system issues. Advice and guidance on using software packages should be sought from a competent person.

Responsibilities

The Clerk is responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Council business.

Users of removable media must have adequate Records Management / Information Security training to enable relevant policies are implemented.

Incident Management

It is the duty of all employees and agents of Council not to allow storage media to be compromised in any way whilst in their care or under their control. There must be immediate reporting of any misuse or irresponsible actions that affect work data or information, any loss of material, or actual, or suspected breaches in information security to the Clerk.

It is the duty of all Councillors/Employees to report any actual or suspected breaches in information security to the Clerk.

Data Administration

Removable media should not be the only place where data created or obtained for work purposes is held, as data that is only held in one place and in one format is at much higher risk of being unavailable through loss, destruction or malfunction of equipment, than data which is routinely backed up.

Where removable media is used to transfer material between systems then copies of the data should also remain on the source system or computer, until the data is successfully transferred to another computer or system.

Where there is a business requirement to distribute information to third parties, then removable media must only be used when the file cannot be sent or is too large to be sent by email or other secure electronic means.

Transferring material to removable media is a snapshot of the data at the time it was saved to the media. Adequate labelling must be undertaken to easily identify the version of the data, as well as its content.

Files must be deleted from removable media, or the removable media destroyed, when the operational use of the material has been completed. Council's retention and disposition schedule must be implemented by Councillors, employees, contractors and agents for all removable media.

Security

All storage media must be kept in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption of the business asset. Due to their small size there is a high risk of the removable media being mislaid lost or damaged, therefore special care is required to physically protect the device and the data. Anyone using removable media to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Virus Infections must be prevented from damaging Councils computer. Virus and malware checking software, approved by Council, must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by the virus checking software, before the media is loaded on to the receiving machine.

Any memory stick used in connection with Council equipment or to store Council material should usually be Council owned. However, work related data from external sources can be transferred to the Council laptop using memory sticks that are from trusted sources and have been checked using current anti-virus software.

Council will not provide support or administrator access for any non-Council memory stick.

Use of removable media

Care must be taken over what data or information is transferred onto removable media. Only the data that is authorised and necessary to be transferred should be saved on to the device.

Council material belongs to Council and any equipment on which it is held should be under the control of the Council and not available to be used for other purposes that may compromise the data.

All data transferred to removable media should be in accordance with an agreed process established by Council so that material can be traced.

The person arranging the transfer of data must be authorised to make use of, or process that data.

Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.

If encryption is available it should be applied to the data file unless there is no risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage. If encryption is not available password control must be applied if removable media must be used for the business purpose.

Faulty or Unneeded Storage Devices

Damaged or faulty media must not be used. The Clerk must be consulted over any damaged equipment, peripherals or media.

All unneeded or faulty storage devices must be dealt with securely to remove the data before reallocating or disposing of the device.

Breach procedures

Users who do not adhere to this policy will be dealt with through Councils disciplinary process.

Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

Review and Revision

This policy will be reviewed annually by Council and revised according to developments in legislation, guidance, accepted good practice and operational use.

Employees Guide in Brief

Data and information are valuable and must be protected.

Only transfer data onto removable media, if you have the authority to do so.

All transfer arrangements carry a risk to the data.

Run the virus checking programme on the removable media each time it is connected to a computer.

Only use approved products for Council data.

Activate encryption on removable media wherever it is available and password protection if not available

Data should be available for automatic back up and not solely saved to removable media.

Delete files from removable media, or destroy the media, after the material has been used for its purpose.

Clerk to Buckland Parish Council

Telephone: 01737 448023 Email: parishcouncil@bucklandsurrey.org.uk

Adopted: 11th May 2026 **Next Review date: May 2027**

Disclaimer: *Hardcopies of this document are considered uncontrolled. For the latest version please refer to www.bucklandsurrey.org.uk*