Pontesbury Parish Council IT Policy

1.Introduction

Pontesbury Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

2. Scope This policy applies to all individuals who use Pontesbury Parish Council's IT resources, including computers, internet access, networks, software, devices, data, and email accounts, webmail, parish council website.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors who use IT systems to carry out council business, whether on council-owned or personal devices.

4. Device and software usage Authorised encrypted devices, software, and applications will be provided by Pontesbury Parish Council staff for work-related tasks. If a member of staff leaves the laptop should be returned to the Clerk on the last day of office. Such laptops and any laptops replaced will have the data removed and destroyed securely by Shroptech.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Council computer equipment/software is provided for council purposes, however reasonable personal use is permitted. Any personal use of our computers and systems should not interrupt our daily council work in any way or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing illegal or discriminatory content.

Locking computers when leaving desk, all councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

Equipment should not be dismantled or reassembled without seeking advice.

Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Clerk.

Any faults or necessary repairs must be reported to Shroptech.

The Council recognises that councillors and staff may wish to use their own smartphones, tablets, laptops, etc to access council emails/papers. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

All councillors should use effective anti-virus and firewall for their personal computer/device that they use for council business. All councillors will use an email address specifically for council business, they will not use their own personal email addresses to conduct council business.

If staff are using mobile phones for work purposes, they must not contain illegal or discriminatory content. Any emails for work purposes, sent from personal devices should be sent from a council email account and should not identify the individual's personal email address.

Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

5. Data management and security All sensitive and confidential Pontesbury Parish Council data should be stored and transmitted securely using approved methods. All parish council staff should 'Restart' their computers weekly to allow for updates. Parish council staff and Chair laptops will be backed up daily through Microsoft 365 and offline quarterly and essential updates installed – by Shroptech.

The security procedures will provide preventative measures to reduce the risks to the system, the information held within the system and the service it supports. Business grade firewalls are deployed at all external gateways of the network and a business grade antivirus application deployed across entire network including servers and endpoints.

The cloud service provider (Microsoft) backs up data necessary to run the council business at least every 7 days and is replicated at a minimum of 2 datacentres. Data is backed up offline quarterly and this is stored in an environment completely separate to the council's network. The council installs critical patches within 30 days of release.

External systems used for payroll (Brightpay) and accounting (Scribe – Starboard Systems) are web-based, backed up at least every seven days and all data is encrypted during transit. Remote access and administrative passwords are high strength, restricted to key personnel and centrally

managed and secured with PBKDF2. Scribe is hosted in Amazons ISO27001 certified data centre in London. The payroll company keep our details for six years following switching payroll company. Scribe give read-only access to our data following switching to different software.

A Continuity plan will be developed and maintained for each system to ensure the principles are sustained and enable the continuation of services following failure or damage to systems or facilities.

The Clerk will be responsible for the implementation and promotion of the procedures.

All parish council staff computerised information systems will be password controlled and all passwords will be treated with the strictest confidence and users will not divulge their password to any unauthorised person. All sensitive data will be password protected. Staff computers all have adequate security software and encrypted hard drives and have business standard antivirus software/Firewall installed.

Any laptops/computers used by the parish council chair and councillors who undertake internal checks or authorise council banking payments will also have their hard drives encrypted and advice given about business grade anti-virus/Firewall software.

When working remotely, users should follow the same security practices as if they were in the office.

All portable computers must be stored safely and securely when not in use in the office. Portable equipment (unless locked in an office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles.

When using personal devices for council business

- secure wifi networks must be used
- users must ensure that work-related data cannot be viewed or retrieved by family or friends that may use that device
- users must inform the Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is a risk of access to personal data relating to council work.

Any media or IT equipment disposed of by the Council will not contain any data or codes that could allow an individual to be identified from it. The disposal of equipment will be made under a controlled and documented environment satisfying the requirements of the Data Protection Act 2018. The disposal of media such as disks and memory sticks must ensure that data cannot be recovered. Disposal of such media through the "everyday" waste collection is not permitted.

The Council will implement processes to ensure appropriate disposal of such media. An inventory of all Council computer equipment will be maintained. Details of any equipment or media disposed of or relocated (other than portable equipment) must be recorded.

6. Network and internet usage Pontesbury Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Staff use a shared network for files, other than Personnel documents which are only viewed by Clerk/Deputy Clerk. Downloading and sharing copyrighted material without proper authorisation is prohibited.

Chair keeps a copy of all passwords for council use in a sealed envelope. In the event of no member of parish council staff being available, this envelope can be opened in the presence of another councillor.

7. Email communication All official emails about council business must come from a council-owned email address e.g. clerk@pontesbury-pc.gov.uk) Email accounts provided by Pontesbury Parish Council are for official communication only. Council emails should not be forwarded to personal email inboxes. Emails should be professional and respectful in tone and not contain illegal or discriminatory content. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links. IT security training will be offered to parish council staff and councillors regularly.

In the event of staff sickness, access will be arranged for staff email accounts by the senior member of staff present at work.

All email communication with suppliers/contractors should only follow agreement by full council, an appropriate committee with delegated powers or by Clerk as governed by Financial Regulations adopted by the council.

When a member of staff or Councillor leaves the council access is removed for their council email address

10. Email monitoring, retention and archiving Pontesbury Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

Emails should be retained and archived in accordance with legal and regulatory requirements (see Information Retention policy adopted by the council). Regularly review and delete unnecessary emails to maintain an organised inbox.

8. Password and account security Pontesbury Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security. Parish council staff and councillors are given annual training on what length and form a password must be by Shroptech.

9. Data protection and GDPR Personal data must not be stored unencrypted on USB sticks, personal laptops, or cloud services like Dropbox unless approved by the council.

The council is a Data Controller and Processor and has appointed a Data Protection Officer who is John Henry of JDH Business Services Ltd. John@Jdhbs.co.uk

This policy should be used and read in conjunction with the parish council Data Protection Policy (which references the requirements when processing personal data for the council) which is available from the Clerk.

If a Freedom of Information request or Subject Access Request (SAR) is received please contact the Clerk immediately. The Clerk will then work with the Data Protection Officer to satisfy the request.

10. Reporting security incidents All suspected security breaches or incidents should be reported immediately to the Clerk/Deputy Clerk (who will contact the Data Protection Officer) for investigation and resolution. Report any email-related security incidents or breaches to the Clerk/Deputy Clerk immediately.

11. Website Management and Accessibility The parish council website must meet WCAG 2.2AA standards and publish all required documents. This is the responsibility of the Clerk working with the website hosts who are Information Solutions/Web Orchard based in Shrewsbury. Contact is Peter White. peter.white@info-sol.co.uk

The website should also satisfy the requirements of the Transparency Code. This is also the responsibility of the Clerk.

12. Training and awareness Pontesbury Parish Council will provide regular training (including at induction for staff and councillors) and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

13. Compliance and consequences Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

14. Health and safety

Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

The 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. Further details are set out in the council's Employee Handbook and Health and Safety Policy.

Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Clerk.

If any hazards are detected at a workstation, including ‘noises’ from the IT equipment, this should be reported immediately to Shroptech.

15 . Policy review This policy will be reviewed annually by the Clerk and councillors to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

17. Contacts For IT-related enquiries or assistance, staff and councillor users can contact the Clerk or Greg Lawrence at Shroptech. greg@shroptech.com

All staff and councillors are responsible for the safety and security of Pontesbury Parish Council’s IT and email systems. By adhering to this IT and Email Policy, Pontesbury Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Date adopted: _____

Date of next Review: _____