Pontesbury Parish Council

INFORMATION SECURITY POLICY

PRINCIPLES & PURPOSE

This Policy sets out the Council's commitment to information security within the Council and provides clear direction on responsibilities and procedures.

Pontesbury Parish Council is a Data Controller, as defined under the Data Protection Act 2018, and has registered as such with the Information Commissioner's Office.

PROTOCOLS

System Security Processes and Procedures

The Council will provide and maintain security processes and procedures for all key information systems. The procedures will uphold the principles of confidentiality, integrity, availability and suitability and be assessed for their impact upon other systems and services.

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.

Physical Security

Adequate and practical access controls will be provided in all areas in which personal and business data is stored or used. Unattended rooms should be secured at all times with locked doors as a minimum security requirement. Computers should be locked when not in use or left in the office.

All documents disclosing identifiable information will be transported in sealed containers eg envelopes.
Within their level of authority, staff will be responsible for minimising the risk of theft or vandalism of the data and equipment through common-sense precautions. In particular high value equipment such as, laptop computers, should not be left unattended or unsecured and paper records should not be left in public view.

The physical environment in which data and equipment is stored will be suitable and fit for purpose to ensure the safety of the data and equipment.

Logical Security
All computerised information and systems are regularly backed up to a secure environment online and quarterly are backed up offline by Shroptech using external hard drives.

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.

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.

Copyright and licences
The Clerk is responsible for ensuring all computer software packages and non-electronic media for use within an information environment are used in accordance with the terms and conditions of use as set out in the licence agreement.

Disposal and movement of equipment and media
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.

Personal Computers
Computer users have responsibility for the security of the equipment in their care and shall not commit an act to compromise the data or Information Security Policy. Staff use PC computers only for council business.

Computer users will be made aware of their responsibilities through this policy

Staff and Councillors' Responsibilities
The Council will make every reasonable effort to ensure that staff and councillors are aware of their responsibilities for the security of information. However, each councillor or member of staff is responsible for ensuring that Security Policy is adhered to and report any breaches of security.
Cyber security training will be provided for all councillors and updated when necessary. Training was offered to councillors in June 2022. Training for staff and councillors who didn't attend in June, in December 2022.

Incident Reporting
Incidents affecting security must be reported to the Clerk as quickly as possible.

Adopted: 11 June 2018
Reviewed: 12 December 2022
Next review date: December 2023