

# PITSTONE PARISH COUNCIL

## Management of Data Policy

### 1. 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 the Council).

Information is used throughout the Council and is sometimes shared with external organisations and applicants. The use of insecure 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 the 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 the Council that the availability, integrity, and confidentiality of all storage devices are maintained at a level which is appropriate to the Council's needs.

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

- Enabling the correct data to be made available where it is required
- Maintaining the integrity of the data
- Preventing unintended consequences to the stability of the computer network
- Building confidence and trust in data that is being shared between systems
- Maintaining high standards of care towards data and information about individual parishioners, staff or information that is exempt from disclosure
- Compliance with legislation, policies, or good practice requirements

### 2. Application of this policy

This policy applies primarily to the Parish Council, although elements may be utilised by the Recreation Ground Charity and Pitstone Parish Charity where appropriate.

### 3. Principles

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

The policy applies to fixed media within devices (for example Laptop hard drives, Tablet internal storage, Mobile Phone internal storage etc) and removable media.

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.

It is the responsibility of councillors and staff to satisfy themselves that they understand nature, and sensitivity, of the information they are storing.

Some information, such as agendas and minutes, are in the public domain and do not require special handling. Other information may be commercially sensitive, relate to private individuals, or be subject to other legal restrictions. This information must be stored in encrypted form.

Where possible all council data stored on fixed media devices should be encrypted. Most laptops, tablets, phones etc will allow this.

Where full encryption of devices is not possible the council will supply an encrypted USB memory stick which MUST be used for all sensitive information. Upon leaving the council, this USB stick, along with any other council property, must immediately be returned to the parish clerk.

Any person who intends to store Council data must abide by this Policy. This requirement devolves to Councillors, employees, and agents of the 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.

#### **4. Advice and assistance**

The clerk will ensure that everyone that is authorised to access the 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 also sort from a competent person. For matters relating to Council data or equipment, please contact the Parish Council IT representative in the first instance.

#### **5. Responsibilities**

Clerks are 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 so that relevant policies are implemented.

#### **6. Incident management**

It is the duty of all employees and agents of the Council to not 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.

#### **7. 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. The Council's retention and disposition schedule must be implemented by Councillors, employees, contractors, and agents for all removable media.

## **8. 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 the Councils network and computers. Virus and malware checking software approved by the 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 network using memory sticks that are from trusted sources and have been checked using current anti-virus software.

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

Any loss of Council owned USB sticks or any other equipment/files containing Council data, must immediately be reported to the Parish Clerk.

## **9. 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 the 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 the Council so that material can be traced.

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

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

Encryption must 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, then password control must be applied if removable media must be used for the business purpose.

**10. 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.

**11. Breach procedures**

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

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

All data breaches, or losses, must be reported immediately to the Parish Clerk.

**12. Guide in brief**

- Data and information are valuable and must be protected.
- If possible, encrypt all devices where council data is stored
- Only transfer data onto removable media if you have the authority to do so and only transfer data onto encrypted media
- 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.

**13. Review**

This policy was adopted by Pitstone Parish Council on .....29/8/24.....

minute reference ...132/24.2..... and will be reviewed on at least an annual basis.

Signed on behalf of Pitstone Parish Council by

*D Nicholls*

\_\_\_\_\_

Chairman