BIGGLESWADE TOWN COUNCIL

Removable Media Policy

This document will be distributed to:

Name

Job Title

Email Address

Contents

1. Policy Statement

Biggleswade Town Council will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.

2. Purpose

This document states the Removable Media policy for Biggleswade Town Council. The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of Wokingham Borough Council's computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

3. Scope

This policy applies to all Members, Committees, Services, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Biggleswade Town Council information, information systems or IT equipment and intends to store any information on removable media devices.

4. Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the Council to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

5. Risks

Biggleswade Town Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business. Information is used throughout the Council and sometimes shared with external organisations and applicants.

Securing **PROTECTED or RESTRICTED** data is of paramount importance – particularly in relation to the Council's need to protect data in line with the requirements of the Data Protection Act 1998.

Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the Council.

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

This policy aims to mitigate the following risks:

- Disclosure of **PROTECTED** and **RESTRICTED** information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of Council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6. Applying the Policy

6.1. Restricted Access to Removable Media

It is Biggleswade Town Council policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the Town Clerk for **Approval.**

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

6.2. Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by the Council's outsourced IT provider. Non-council owned removable media devices must not be used to store any information used to conduct official Council business, and must not be used with any Council owned or leased IT equipment.

The only equipment and media that should be used to connect to Council equipment or the Council network is equipment and media that has been purchased by the Council and approved or has been sanctioned for use by the Council.

6.3. Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore, removable media should not be the only place where data obtained for a council purpose is held.

Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all **PROTECTED or RESTRICTED** data held must be encrypted.

Users should be aware that the Council will audit / log the transfer of data files to and from all removable media devices and Council-owned IT equipment.

6.4. Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to the Town Clerk.

It is the duty of all Members to report any actual or suspected breaches in information security to the Chairman of the Council.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident.

6.5. Third Party Access to Council Information

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from the Council's network, information stores or IT equipment without explicit agreement from the Council's outsourced IT provider acting on behalf of Biggleswade Town Council.

Should third parties be allowed access to Council information then all the considerations of this policy apply to their storing and transferring of the data.

6.6. Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the Council's outsourced IT provider should removable media be damaged.

Virus and malware checking software approved by the Council's outsourced IT provider 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 two functionally different virus checking software products, before the media is loaded on to the receiving machine.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage.

6.7. Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the Council or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to the Council's outsourced IT provider for secure disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the Council's outsourced IT provider.

6.8. User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with Council equipment or the network or to hold information used to conduct official Council business must only be purchased and installed by the Council's outsourced IT provider. Any removable media device that has not been supplied by IT must not be used.

- All data stored on removable media devices must be encrypted where possible.
- Virus and malware checking software must be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices 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.

For advice or assistance on how to securely use removable media devices, please contact the Council's outsourced IT provider.

7. Policy Compliance

If any user is found to have breached this policy, they may be subject to Biggleswade Town Council's disciplinary procedure.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

8. Policy Governance

The following table identifies who within Biggleswade Town Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amends.
- Informed – the person(s) or groups to be informed after policy implementation or amends.

Responsible

Town Council and Committees.

Accountable

Town Clerk.

Consulted

Town Councillors and Committee Members.

Informed

All Council Employees, All Temporary Staff, All Contractors.

9. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.