West Dunbartonshire Council

USB Data Drive Policy

Contents

1. Background

1.1 West Dunbartonshire Council ('the Council') recognises the benefits of mobile and flexible working and the increasing need for collaboration both in and out-with the office. Whilst the Council recognises that removable media such as USB data drives can enhance collaboration and productivity by making it easier to work when outside of the office environment, it also recognises that this presents additional risk.

1.2 This Policy will clarify in which scenarios removable media should be used, identify alternative ways of working and ultimately minimise/remove the need and potential risk of such usage.

2. Scope

2.1 This Policy applies to all users who have access to ICT resources provided by the Council, meaning all:

- Employees;
- Trade Union representatives (including those not directly employed if using the Council's ICT resources);
- Elected Members;
- Agency workers;
- Suppliers/Contractors/subcontractors (subject to any relevant provision in their contracts);
- Employees of trusts, agencies and companies that use the Council's ICT resources;
- Students and volunteers (where undertaking work experience or similar);
- Partner organisations; and
- Any other person(s), without exception, who uses or requires access to Council owned or leased ICT equipment, systems and networks.

3. Purpose

3.1 The use of removable USB data drives comes with additional security and data challenges and risks, as they are easily lost or stolen. These devices can also infect PC's and networks by transferring malware and viruses, particularly when being used to go between non trusted devices (such as personal devices, mobile) and trusted devices (such as Council devices) or networks.

3.2 This Policy is required to clarify the permissible usage situation for USB data drive access, promote alternative solutions (where possible) and outline situations where USB data drive access is not permissible.

4. Unacceptable use

4.1 There are no circumstances where you can use an unauthorised USB data drive to undertake work on behalf of the Council or connect such a device to the Council network, nor should you allow anyone else to do so using your device. An unauthorised device is a device that has not been procured via the appropriate purchasing mechanisms within the Council and examples include personal USB data drive or one provided by a third party such as a supplier, or charging personal mobile phones via a Council USB port.

4.2 Under no circumstances should you connect any 'found' USB data drives to a Council device or to the Council network. The content will be unknown and connecting to a Council device or the Council network introduces the potential for malware. Any such devices should be passed to the ICT service desk for investigation.

4.3 The content of paragraphs 4.1 and 4.2 are also covered in Appendix 1 – part 2 item 7 of the Acceptable Use Policy. Any contravention of the above items may be considered a breach of the policy and be subject to investigation as detailed at section 8 of this policy.

4.4 Suppliers, consultants and trainers should be advised to contact ICT in advance to discuss and arrange suitable alternate solutions to using USB drives.

5. Safe use

5.1 All requirements for USB use including emergency situations must be raised via a change request on the ICT helpdesk system for investigation and where appropriate authorised via ICT Security.

5.2 All USB drives must be purchased via the appropriate purchasing process within the Council.

5.3 All USB drives must be encrypted in accordance with the latest standards and advice provided by ICT.

5.4 All data being processed on behalf of the Council must be in the password-protected area of the encrypted USB drive.

5.5 If there is any suspicion that a USB drive have been exposed to malware, then the ICT service desk must be advised and the drive handed over to them for scanning and retrieval of any data.

5.6 Users should be aware of the risk to their own personal data and personal devices. Users should maintain anti-virus software on any personal devices likely to be used with a Council USB drive.

5.7 In very limited circumstances, the connection of USB devices (such as a CD/DVD blower/reader) may be required for specific purposes by specific service areas; this must be agreed with ICT security in advance.

6. Future use

6.1 ICT will install a monitoring technology to alert when a USB port has been used. The user will then be contacted to discuss and agree a different solution to meet their business need. The user must thereafter use the new solution.

6.2 Users who currently have USB drives (authorised and unauthorised) can hand these to ICT for checking and safe disposal of both the data and the USB drives. The data requirements will be discussed with the user and where required extracted and secured appropriately.

6.3 USB drives should only be used when no alternative solution has been identified.

6.4 The requirement to use USB drives should be limited.

6.5 Users wishing to use USB drives should contact the ICT service desk for advice on alternatives.

6.6 Users will be guided to always consider alternative means of accessing council resources before resorting to USB drives, for example:

- Access resources via thin client technology which allows for ‘Use Your Own Device’ provision. This delivers a secure connection to the Council’s thin client environment with the appropriate internet connection;
- Access via the Council’s Ourcloud environment;
- Ask suppliers to email course and seminar presentations rather than issue on USB; and
- Contacting the ICT service desk to transfer data from USB on the behalf of Users, Suppliers or Third Parties
- Email documents /files via the council secure email facility which is automatically virus checked.

7. Monitoring

7.1 All USB drives in use across the Council must be authorised devices only, procured via the ICT catalogue or on advice.from the ICT service desk or relevant ICT employees.

7.2 USB drives should be considered an Asset and recorded in each service areas Asset inventory.

7.3 Service areas should record who has the USB drives, for what purpose and for what type of data.

8. Breach reporting and consequences of misuse

8.1 The reporting of breaches would be undertaken in accordance with the Reporting of Information security concerns as part of the ICT Security framework which can be found here.

8.2 Potential consequences of misuse will be handled in accordance with the Acceptable Use Policy as part of the ICT Security framework which can be found here.

9. Lost USB data drives and virus warnings

9.1 If your USB drive is lost and contains information of a personal/sensitive nature, you must notify your line manager immediately and subsequently report the loss via the DPA/GDPR guidance.

9.2 If you plug the USB device into a council computer/device and the computer returns a message advising that the drive is infected with malware, you must immediately remove the drive from the computer and report the incident to the ICT service desk.

10 Clarification

10.1 In the event of an issue arising from an interpretation of this Policy, content clarification should be sought from the ICT Security Officer in the first instance either by email or by telephoning 01389 737568, or by raising a request with the ICT service desk.

11 Version Awareness

11.1 The audience of this document should be aware that a physical copy might not be the latest available version. The latest version, which supersedes all previous versions, is available on the Council Intranet. Those to whom this Policy applies are responsible for familiarising themselves periodically (minimum annually) the latest version and for complying with the Policy.

11.2 This policy will be reviewed regularly or as and when significant applicable technological changes are introduced.