PSPS

Public Sector Partnership Services Ltd

Delivering services for South Holland District Council, Boston Borough Council, East Lindsey District Council

Appendix B

Information Security Policy Removable Media

May 2021

Document Control

Version Control

Issue Number	Issue Author	Issue Date	Reason for Issue
2.0	J Wright	Oct-18	Review & refresh of current policy
2.1	J Wright	Feb-19	Rebrand
3.0	J Wright	Feb-21	Periodic review
3.1	J Wright	May-21	Review to include Boston Borough Council

Approval Control

Issue Number	Approval Authority	Name	Approval Date	Due for Review
3.1	ELDC/BBC	James Gilbert	May-21	May-24
	PSPS	Lewis Ducket	May-21	May-24
3.2	SHDC	James Gilbert		May-24

Contents

1. Policy Aim 4

2. Introduction 4

3. Roles and Responsibilities 5

4. Definition 5

5. Policy Statement 5

5.1 Procurement of Removable Media 6

5.2 Security of Data 6

5.3 Incident Management 6

5.4 Disposing of Removable Media Devices 7

6 Review 7

7 Policy Compliance 7

8 Related Policies 7

1. Policy Aim

The aim of this Policy is to define the broad mechanisms and roles through which the Organisation will be able to demonstrate accountability and compliance with regards to Removable Media.

Responsible	Head of ICT & Digital
Accountable	Chief Executive (PSPS), Executive Director (SHDC), Assistant Director (ELDC/BBC)
Consulted	Data Protection Officers, ICT Security Lead
Informed	All ICT Users

2. Introduction

This is a joint Removable Media Policy. Where “The Organisation” is referenced, this refers to either Public Sector Partnership Services or its Client Council’s South Holland District Council, East Lindsey District Council or Boston Borough 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 the 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.

This policy applies to Councillors, employees, contractors, consultants, temporaries, and other workers at the Organisation, including all personnel affiliated with third parties.

This Removable Media Policy forms part of the Information Security Framework.

3. Roles and Responsibilities

The following roles are those formally defined within the Policy:

Role	Responsibility
The Organisation's Chief Executive	Supporting Company/Authority compliance with the policy
Senior Management Team	Ensuring the policy adheres to statutory legislation & guidance and that it is embedded in the workforce and ensuring managers and Team Leaders show compliance with the policy and it is understood.
Managers & Team Leaders	Understanding and complying with the policy, ensuring it is available to team members, and advising on it.
All Staff	Understanding and complying with the policy.

4. Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the Organisation 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
- Smart Phones

5. Policy Statement

It is the Organisation's policy to prohibit the use of all removable media devices wherever possible. The use of technical controls will be used to enforce this policy.

The use of removable media devices will only be granted if approved by a Manager and upon acceptance of the associated risks.

Requests for access to, and use of, removable media devices must be made to the ICT Service Desk. Approval for their use must be given by the ICT Security Analyst.

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

5.1 Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by the ICT Department. Non-Organisation owned removable media devices must not be used to store any information used to conduct official business, and must not be used with any Organisation owned or leased ICT equipment without having been virus checked by the ICT Section.

Only removable media that has been purchased by the Organisation and approved by the ICT Department is authorised for use.

5.2 Security of Data

Removable Media should be considered a secondary copy of the data and is not to be the only place where data obtained for business purposes 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 should, where possible be encrypted. If this is not possible, then all personal or confidential data held must be encrypted.

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

5.3 Incident Management

Virus and malware checking software approved by the ICT team 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 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 company, other Organisation's or individuals from the data being lost whilst in transit or storage.

It is the duty of all users to immediately report any actual or suspected breaches in information security to the ICT Service desk as referenced in the Information Security Incident Management Policy who will carry out the process as outlined in the Incident Management Policy.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the IT Service desk as referenced in the Information Security Incident Management Policy.

5.4 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 company 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 ICT Service desk for secure disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the ICT Service desk.

6 Review

As a standard principle, this policy should be reviewed at least once every two years to ensure that it remains fit for purpose. It may need reviewing more regularly in response to specific legislation changes or changes to best practice guidance.

7 Policy Compliance

If any user is found to have breached this policy, they will be subject to the Organisation'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).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Department.

8 Related Policies

ICT Incident Management Procedure

Employers Code of Conduct