Policy Document

Removable Media Policy

[23/08/2011]

Document Control

Redditch Borough Council
Removable Media Policy
Mark Hanwell
Removable Media Policy.doc
Mark Hanwell – ICT Transformation Manager
[Communications and Operation Management Policy
[Marking Classification]
23/08/2011

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Head of Business Transformation	Deborah Poole	23rd August 2011

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contents

1 Policy Statement

Redditch Borough 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 Redditch 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 Redditch 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 Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Redditch Borough 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

Redditch Borough 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 PROTECT 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 PROTECT 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 Redditch Borough Council's policy to prohibit the use of all removable media devices except those that are pre-authorised. 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 ICT Helpdesk. Approval for their use must be given by your line manager.

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. 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 by the ICT Manager or has been sanctioned for use by the ICT Manager.

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 Council 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. For further information please see Remote Working Policy and Communications and Operation Management Policy].

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 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, including Council Members, to immediately report any actual or suspected breaches in information security to the ICT Helpdesk.

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

6.5 Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the ICT helpdesk should removable media be damaged.

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.

6.6 Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be returned to ICT for disposal.

7 Policy Compliance

If any user is found to have breached this policy, they may be subject to Redditch Borough 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).

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

8 Policy Governance

The following table identifies who within Redditch Borough 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 amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ICT Transformation Manager
Accountable	Head of Business Transformation
Consulted	Corporate Management Team
Informed	All Council employees, councillors, all temporary staff, all contractors etc

9 Review and Revision

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

10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document.

- Legal Responsibilities Policy.
- Remote Working Policy.
- Information Security Incident Management Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy.

- Email Policy.
- Internet Acceptable Use Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- IT Access Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- IT Infrastructure Policy.
- Communications and Operation Management Policy.

11 Key Messages

- It is Redditch Borough Council's policy to prohibit the use of all removable media devices except those pre-authorised by ICT. The use of removable media devices will only be approved if there is a valid business case for its use.
- Any removable media device that has not been supplied by ICT **must not** be used.
- Damaged or faulty removable media devices must be returned to ICT.
- 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.