BOLSOVER DISTRICT COUNCIL

Removable Media Policy

January 2011

This Policy addresses the following Corporate Aims (show those which are appropriate to the policy only):

COMMUNITY SAFETY

CUSTOMER FOCUSED SERVICES

ENVIRONMENT

REGENERATION

SOCIAL INCLUSION

STRATEGIC ORGANISATIONAL DEVELOPMENT

Bolsover District Council Equalities Statement

Bolsover District Council is committed to equalities as an employer and in all the services provided to all sections of the community.

 The Council believes that no person should be treated unfairly and is committed to eliminate all forms of discrimination in compliance with the Equality Strategy.

 The Council also has due regard to eliminate racial discrimination and to proactively promote equality of opportunity and good relations between persons of different racial groups when performing its functions.

This document is available in large print and other formats from any of the Council offices or by contacting the Chief Executives Directorate on 01246 242323. Please bear in mind we will need a few days to arrange this facility.

If you need help to read this document please do not hesitate to contact us.

Our Equality and Improvement Officer can be contacted via **Email** or by telephoning 01246 242407.

Minicom: 01246 242450
Fax: 01246 242423

CONTROL SHEET

Details of Document	**Comments / Confirmation**
Title	Removable Media Policy
Document type – i.e. draft or final version	Draft
Location of Policy	Intranet
Author of Policy	Business Development Manager
Member route for Approval & Cabinet Member concerned	Improvement Scrutiny, Executive. Portfolio Holder for Efficiency
Date Risk Assessment completed	
Date Equality Impact Assessment approved	Submitted to CSPD
Partnership Involvement (if applicable)	Developed from the Policy at North East Derbyshire District Council
Date added to the Forward Plan	
Policy Approved by	
Date Approved	
Policy Review Date	
Date forwarded to CSPD (to include on Intranet and Internet if applicable to the public)	

CONTENTS

1 Policy Statement

Bolsover District Council will ensure the controlled use of removable media devices (see section 4 below for definition) 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 Bolsover District 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 Bolsover District 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 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 Bolsover District Council information, information systems or IT equipment and intends to store any information on removable media devices.

4 The Policy

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

Bolsover District 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 RESTRICTED (see definition in section 12) 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 (see the Regulatory and Compliance Policy). 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 RESTRICTED information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of Council's networks or equipment through the introduction of viruses through the transfer of data from one form of 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.
- Loss of intellectual property.

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 Bolsover District Council policy to restrict and control 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 ICT Service Desk. Approval for their use must be given by the Information Security 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 and installed by the ICT Service. 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. Appropriate training in the usage of devices will be given by the ICT Section upon issue.

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 Information Security Manager or Senior Information Risk Owner (**SIRO**).

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 Information Handling & Protection 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, where possible, be encrypted. If this is not possible, then all RESTRICTED data held must be encrypted.

Users should be aware that the Council may 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 ICT Servicedesk or Information Security Manager and if this involves any personal information, as defined by the Data Protection Act, it must also be reported to the Data Protection Officer.

It is the duty of all councillors to report immediately any actual or suspected breaches in information security to the ICT Servicedesk or Information Security Manager and if this involves any personal information, as defined by the Data Protection Act, it must also be reported to the Data Protection Officer.

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

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 network, information stores or IT equipment without explicit agreement from the Information Security Manager or Senior Information Risk Owner (**SIRO**).

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 and may be subject to a formal exchange agreement between concerned parties.

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 ICT Servicedesk should removable media be damaged.

Virus and malware checking software approved by the Information Security Manager 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 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, have become damaged, or are returned as part of the exit procedure, must be securely wiped, or disposed in a manner such that reconstruction of data is highly unlikely, in order 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, have become damaged, or are to have data securely erased, must be returned to the ICT Servicedesk for secure disposal, or erasure.

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 ICT Servicedesk. 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 has been authorised in the Business Case and is 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 ICT Servicedesk.

7 Policy Compliance

If any user is found to have breached this policy, they may be subject to Bolsover District Council 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 Human Resources.

8 Policy Governance

The following table identifies who within Bolsover District Council is Accountable, Responsible, Informed or Consulted with regards to this policy.

Responsible (the person(s) responsible for developing and implementing the policy)	Information Security Manager.
Accountable (the person who has ultimate accountability and authority for the policy)	Section 151 Officer
Consulted (the person(s) or groups to be consulted prior to final policy implementation or amendment)	Internal Audit
Informed (the person(s) or groups to be informed after policy implementation or amendment)	Bolsover District Council Employees, Bolsover District Council Members, 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.

Policy review will be undertaken by the Information Security Manager.

10 References

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

- Information Handling and Protection Policy – to be developed

The following Bolsover District Council policy documents are indirectly relevant to this policy:

- Acceptable Use Policy.
- Business Continuity Management Policy.
- Information Handling and Protection Policy – to be developed
- Information Security Policy.
- Access to data and information policy
- Departmental Data Protection codes.

11 Key Messages

- It is Bolsover District Council policy to restrict and control the use of all removable media devices. 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.
- All data stored on removable media devices **must** be encrypted where possible.
- Damaged or faulty removable media devices must not be used.
- 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.

Removable media devices that are no longer required, or have become damaged, must be disposed of securely by the ICT Servicedesk to avoid data leakage.

12. Definitions

This is information where the release could cause **significant** harm or prejudice to:

- an individual if it contains sensitive personal information
- the Councils, or a third parties, commercial interests
- the investigation or prosecution of a crime, or the apprehension of an offender
- the effective conduct of public affairs

Information Security Manager – The IT Manager for the joint ICT service for Bolsover, Derbyshire Dales and North East Derbyshire District Councils.

Senior Information Risk owner – The Head of Customer Service and Performance