Removable Media Policy
## Version Control

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2013</td>
<td>1.1</td>
<td>Updated following comments from IMG</td>
</tr>
<tr>
<td>November 2013</td>
<td>1.2</td>
<td>Updated following comments from ITPARG</td>
</tr>
<tr>
<td>July 2013</td>
<td>1.3</td>
<td>Updated following comments</td>
</tr>
<tr>
<td>September 2015</td>
<td>1.4</td>
<td>Policy subject to full review</td>
</tr>
<tr>
<td>December 2015</td>
<td>1.5</td>
<td>Draft approved at IMG</td>
</tr>
<tr>
<td>February 2016</td>
<td>1.5</td>
<td>Union Consultation</td>
</tr>
<tr>
<td>March 2016</td>
<td>2.0</td>
<td>Approved by Executive Decision</td>
</tr>
</tbody>
</table>
## Table of Contents

1. Introduction .......................................................................................................................... 4  
2. Policy Statement .................................................................................................................. 4  
3. Scope .................................................................................................................................... 4  
4. Handling Removable Media .................................................................................................. 4  
5. Responsibilities .................................................................................................................... 4  
6. Information Management Group (IMG) ............................................................................. 7  
7. Business IT ............................................................................................................................ 7  
8. Internal Audit ......................................................................................................................... 8  
9. Line Managers ..................................................................................................................... 8  
10. Employees ........................................................................................................................... 8  
11. Review and Governance ...................................................................................................... 8  
12. Policy Compliance ............................................................................................................... 8
1 Introduction

1.1 This Policy establishes the principles and working practices that are to be adopted by all Employees in order for data to be safely stored and transferred on removable media.

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

2 Policy Statement

2.1 The Council will ensure the controlled use of removable media devices to store and transfer information by all Employees who have access to information, information systems and ICT equipment for the purposes of conducting official Council business. It is Council Policy to prohibit the use of all removable media devices unless a valid business case for its use is provided.

2.2 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 Council's network e.g. the introduction of viruses.
- Avoid contravention of any legislation, policies or good practice requirements e.g. the Data Protection Act 1998.
- Prohibit the disclosure of information as may be necessary by law.
- Protect damage to the Council's reputation as a result of information loss or misuse.
- Protect the Council from potential legal action as a result of information loss or misuse.
- Protect the Council from potential sanctions imposed by the Information Commissioner’s Office as a result of information loss or misuse.

3 Scope

3.1 This Policy applies to all Employees and third parties working for or on behalf of the Council who have access to Council information, information systems or ICT equipment and intends to store any information on removable media devices. For the purpose of this Policy the term ‘Employee’ refers to all full-time and part-time employees, temporary employees, agency workers, contractors and consultants.

3.2 This Policy should be read in conjunction with the Code of Conduct, the Council Comprehensive Equality Policy and other associated relevant policies, procedures and guidance as contained within the Information Management Framework.

4 Handling Removable Media

Prohibited Removable Media Devices

4.1 Removable media devices that are prohibited without a valid business case include, but are not restricted, to the following:

- CD’s
• DVD’s
• Bluetooth Device
• Media Card e.g. SD/XD
• External Hard Drives
• USB Memory Sticks (also known as pen drives or flash drives)
• Embedded Microchips (including Smart Cards and Mobile Phone Memory Cards)
• MP3 Players
• Digital Cameras
• Backup Tapes
• Dictation Devices
• Floppy Disk
• Infrared device
• Tape Drive
• Webcam

Restricted Access to Removable Media

4.2 It is Council Policy to prohibit the use of all removable media devices unless a valid business case for its use is provided. 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.

4.3 Requests for access to, and use of, removable media devices must be made by completing the Removable Media Business Case Form, which is contained within the Information Management Framework. Guidance Notes for completing the form are also available.

4.4 The following sections must be adhered to at all times.

Use of Removable Media

4.5 The only devices and media that should be used to connect to Council ICT equipment or the Council network is equipment that has been purchased by the Council and approved using the Business Case process set out in this Policy. ¹

4.6 The Council has obligations under Freedom of Information and Data Protection (including security and retention). Therefore, only Council issued removable media devices must be used to store information used to conduct official Council business.

4.7 Unless approval is granted through the Business Case process set out in this Policy, Council issued removable media devices must not be connected to any device that is external to the Council’s network.

4.8 Removable media devices must only be used for work purposes.

4.9 All costs for removable media and associated devices will be met from Service Departments.

Data Security

4.10 Data that is held only 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 sources system or networked drive until the data is successfully transferred to another networked drive or backup/archive medium.

¹ The only exception to this is if there was no suitable alternative method of accessing the information. The removable media device must be from a trusted source and must be virus-checked on insertion.
4.11 In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

4.12 Removable media devices, and the information stored on these devices, must not be compromised in any way.

Incident Reporting

4.13 Actual or suspected breaches in information security, (including loss or theft of devices) should be reported immediately to the IT Service Desk.

4.14 The Council’s Information and ICT Incident Management Policy should be complied with.

Third Party Access to Council Information

4.15 No third party (including external contractors, partners or agents) may access data or extract information from the Council’s network, information stores or IT equipment without explicit agreement from Business IT and the data owner.

4.16 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.

4.17 Third parties are managed in line with the Council’s Third Party ICT Access Procedure.

Preventing Information Security Incidents

4.18 Damaged or faulty removable media devices must not be used.

4.19 Up to date virus and malware checking software must be used on any device to which the removable media is connected.

4.20 Whilst in transit or storage, the data held on any removable media device must be given appropriate security according to the type of data and its sensitivity.

4.21 Encryption or password controls must always be applied to the data files unless there is clearly no risk to the Council (non-personal/sensitive/confidential data), other organisations or individuals from the data being lost, stolen or damaged whilst in transit or storage.

4.22 Passwords for removable media devices which contain personal/sensitive information should be in line with Council standards and should be stored securely and not with the device.

Disposing of Removable Media Devices

4.23 Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Previous contents of any reusable media that are to be reused 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 Business IT for secure disposal.

USB/CD/DVD Usage

4.24 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 CD’s and DVD’s:

- A usage log of any removal media device must be maintained, including dates/times out/in, Employee requesting, purpose and approved by.
- Any removable media used in connection with Council ICT equipment or the network to hold information used to conduct official Council business must be purchased
through Corporate procurement and installed by Business IT. Any non-Council approved removable media devices must not be used.  

- All personal or sensitive data stored on removable media devices must be encrypted.  
- Virus and malware checking software must be used when the removable media device is connected to a device.  
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted may still be retrieved.  
- Removable media devices must not 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.

**Monitoring Removable Media Usage**

4.25 Use of removable media is logged and interrogated for the purposes of:

- Ensuring compliance with policies and procedures
- Investigating or detecting unauthorised use of Council ICT equipment and network
- Detecting or investigating inappropriate use of Council ICT equipment and network
- Preventing or detecting crime
- Determining if usage is relevant to the business

4.26 Only authorised staff will undertake the monitoring of removable media usage. All violations of the Policy reported to or by Internal Audit will be fully investigated.

### 5 Responsibilities

#### Information Management Group (IMG)

5.1 The role of the Information Management Group (IMG) is to co-ordinate the approach to every aspect of Information Management, and not just compliance with DPA 1998.

5.2 The group is made up of Departmental Information Management Representatives who are senior managers in each Department and are responsible for a multi-disciplinary approach to the management of information throughout their Departments.

5.3 The IMG is responsible for the overarching governance and implementation of the Policy throughout the Council.

5.4 The IMG is responsible for ensuring that all Employees are fully aware of Council policy and process, and have received appropriate training.

5.5 The IMG is also responsible for the development and monitoring of the adherence to the Policy.

#### Business IT

5.6 Business IT has overall responsibility for the issue, management and maintenance of Council removable media devices.

5.7 Business IT will maintain logs required for monitoring purposes.

5.8 Business IT are responsible for processing and approving removable media business cases.

---

2 The only exception to this is if there was no suitable alternative method of accessing the information. The removable media device must be from a trusted source and must be virus-checked on insertion.
5.9 Business IT will provide operational procedures and advice for using removable media devices, virus checking and maintenance.

**Internal Audit**

5.10 Internal Audit has responsibility for monitoring the use of removable media, and investigating any suspected misuse.

**Line Managers**

5.11 Line Manager must authorise business cases and ensure that within their area of responsibilities removable media is only used in accordance with this Policy and defined operation procedures.

**Employees**

5.12 Employees are 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 whilst in their care or under their control.

5.13 Employees using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that reasonable care was taken to avoid damage or loss.

5.14 Employees should immediately report any actual or suspected breaches in information security, (including loss or theft of devices) to the IT Service Desk.

5.15 It is the Employees responsibility contact the IT Service Desk if removable media is damaged.

5.16 Employees must ensure that anti-virus and malware checking software is installed and up to date. If in any doubt, the IT Service Desk should be contacted.

**6 Review and Governance**

**Policy Governance**

6.1 The Policy will be subject to governance through the IMG, and will be formally approved by Chief Officers Group via the Executive Decision Framework.

6.2 The Policy will be subject to at least an annual review, and where changes in legislation require, more frequent.

**7 Policy Compliance**

7.1 If you are found to have breached this Policy, the matter will be considered and investigated under the Council’s disciplinary procedure.

7.2 Serious breaches of this policy may constitute gross misconduct and lead to summary dismissal. Breaches, where applicable, may also result in civil action and/or criminal charges.