South Cambridgeshire District Council

REMOVABLE MEDIA POLICY

DRAFT v0.4

December 2011

CONTENTS

Document Information

Issued By:	Information Management
Policy Approved by:	
Policy Approval Date:	
Status:	Draft to be presented to IGWG
Review Frequency:	Every 2 Years

Version	Date	Summary of Changes
0.1	17th August 2011	First draft
0.2	26th August 2011	Revision - MH
0.3	14th October 2011	Revision – IGWG Consultation
0.4	29th December 2011	Revision – EMT Consultation

1   Introduction

In order to ensure the availability, integrity and confidentiality of all Council data, South Cambridgeshire District Council (SCDC) must control the use of removable media storage devices. This policy must be followed whenever removable media devices are used.

2   Purpose

The purpose of this policy is to define user responsibilities for handling all types of removable media and prevent the unauthorised disclosure, removal, destruction, loss or theft of Council data. This policy aims to ensure that the use of removable media is controlled, in order to:
   • Maintain the integrity and availability of Council data and information
   • Prevent the contravention of legislation, Council policies or good practice requirements
   • Build confidence and trust in the data that is being shared between systems
   • Prevent the disclosure, loss or theft of protectively marked information, and to protect against damage or distress to residents, the Council, its staff, Members or partners.

3   Scope

All staff, Members and contractors working on behalf of the Council who have access to the Council's secure IT network are expected to abide by this policy.

4   Definitions

4.1   Devices/Media
'Removable media' refers to data storage devices which are not fixed inside a computer and can include, but are not limited to:
   • Optical Disks (CDs/DVDs)
   • External Hard Drives
   • USB Memory Sticks (aka pen drives or flash drives)
   • Media Card Readers
   • Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
   • MP3 Players/Recorders
   • Digital Cameras

4.2   Specific Usage
This policy seeks to protect the Council from the risks associated with data being extracted from the network to removable media. This policy does not restrict the use of devices to upload information to the network, such as photographs. Neither does it restrict the practice of using USB ports to recharge batteries of devices.

5   Use of Removable Media

5.1   Purpose
The list of removable media above shows a wide range of devices used to store information for a variety of purposes. Some of these, such as CDs and DVDs are sometimes used for long-term storage of data. In these cases careful consideration must be given to the suitability of the media used for the specific data stored. In all other cases, removable media devices must be considered as temporary storage solutions. Removable media must only be used to store information that is required for a specific business purpose.

5.2   Restricted Access to Removable Media
It is SCDC's policy to restrict the use of removable media devices and the accessibility of these to the council network and ICT hardware. Requests for access by all non-SCDC removable media devices must be made to the ICT Service Desk. In all cases the business benefits must be demonstrated and outweigh any risks involved. ICT Service Desk will

create and maintain a list of approved devices and permissions, and may audit and log the transfer of data files to and from removable media devices.

5.3 Procurement of Removable Media

Only removable media devices, including any associated equipment and software, that have been purchased and supplied by the Council can be used to store data from the council network. Where this is not practicable and externally procured media is required to be used, permission must be sought from the Head of ICT and this must be documented prior to access being granted.

5.4 Security of Data

Users of removable media must take all reasonable steps to protect Council data stored on them. If the data is protectively marked, this must be encrypted in line with the Protective Marking Policy, and securely deleted as soon as the justifiable business need ceases. It is the responsibility of the Information Owner to ensure the correct marking is applied to all data sets, and to manage access to these, as specified by the Data Handling Policy.

5.5 Physical Security

All removable media devices must be kept physically secure at all times. Users must take all reasonable steps to protect devices from loss, damage, or misuse. 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. Devices must never be left unattended in any public place, including in vehicles.

5.6 Remote Working

Staff, Members and contractors requiring remote access to the Council network should do this via VPN access. Where this is not possible, approved removable media may be used to enable processing to be carried out on the data using a device not controlled by the Council (e.g. a home PC or Mac). Data on the removable media should not be copied to the host device, and if this is unavoidable, all data must be encrypted, and removed from the host device as soon as processing is complete.

5.7 Incident Management

All users must report any actual or suspected information security incidents to the ICT Service Desk in accordance with the Information Security Incident Management Policy.

5.8 Disposal of Removable Media Devices

All removable media devices that are no longer required or have become damaged must be returned to the ICT Service Desk for secure disposal. All content of removal media that are to be reused must be erased completely.

6 Further Information

For further advice or assistance on how to use removable media devices, please contact the ICT Service Desk. For advice or assistance on the management and use of data please contact the Information Management team.