Neath Port Talbot
Castell-nedd Port Talbot
County Borough Council Cyngor Bwrdeistref Sirol

Removable Media Policy

Rhos Primary School

Version Control		
Version	**Date**	**Comments**
Version 1	April/May 2008	Initial draft of policy
Version 1.1	June 2009	Union & Personnel comments added
Version 1.2	Jan 2012	Review – small amendments and contacts updated
Version 1.3	June 2013	Review
Version 1.4	October 2014	Review and small amendments
Version 1.5	January 2016	Review and small amendments
Version 1.6	June 2017	Review and small amendments
Version 1.8	May 2018	Review and small amendments

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

REMOVABLE MEDIA POLICY

1. INTRODUCTION 3
2. RISK ASSESSMENT 3
3. MANAGEMENT RESPONSIBILITIES 4
4. USER RESPONSIBILITIES 5
5. INCIDENT REPORTING 6
6. DISCIPLINARY CONSIDERATIONS 6
7. GENERAL QUERIES 7

1. INTRODUCTION

1.1 This document sets out the Authority's policy for the use and security of removable media devices/equipment. It sets out the rules relating to use and the consequences which could arise from misuse.

1.2 The term removable media encompasses:

- USB flash drives/memory sticks
- Writeable and rewriteable CDs/DVDs
- Floppy disks
- Digital cameras
- Memory cards
- MP3/MP4 players
- Mobile 'phones
- Bluetooth/infra-red devices

1.3 This Policy applies to all employees of the Authority, elected members, contractors, agency staff and any others with access to Authority information assets or who use the Authority's IT and communication systems

1.4 The term "*information asset*" is defined as any information of value which is owned and/or used by the authority and can be electronic or non-electronic.

1.5 Information assets are used throughout the Authority and can, at times, be shared with external organisations and service users. Consequently any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the Authority and may result in financial loss and/or an inability to provide services to the public.

1.6 It is therefore essential for the continued operation of the Authority that the availability, integrity and confidentiality of all information assets are maintained at a level, which is appropriate to the Authority's needs.

2. RISK ASSESSMENT

2.1 Prior to approval being given for the use of removable media, a risk assessment should be carried out to determine the fitness for purpose of the device being contemplated.

2.2 Consideration should be given to the type of data which will be stored on the removable media. If the data which is to be held on the media is sensitive then consideration must be given to security of that data e.g. encryption must be considered. Help and advice can be obtained from the Business Relations Manager.

3. MANAGEMENT RESPONSIBILITIES

3.1 Management has a responsibility that, in terms of the use and control of removable storage media, the following principles are adhered to:

- Information is a valuable asset to and of the Authority and the Authority has a duty to protect the asset from unauthorised use, disclosure, access, modification loss or destruction.

- The Authority will abide by legislation and regulations that control the obtaining, processing, use, storage and supply of information to others.

- The Authority will ensure the confidentiality, availability and integrity of data

- The Authority will avoid contravention of any legislation, policies or good practice guidelines

- The Authority will maintain high standards of care in ensuring the privacy of personal, third party, privileged and confidential information

- The Authority will prevent unintended consequences to the stability and integrity of the computer network

- To prevent disclosure of sensitive or business orientated data to unauthorised persons all electronic hardware must undergo data eradication prior to disposal. This can be carried out within the Authority or by a contracted third party.

3.2 Management should ensure that when employees terminate employment or transfer posts removable media related to the post is dealt with appropriately.

4. USER RESPONSIBILITIES

4.1 Each member of staff is responsible for the appropriate use and security of data and for not allowing removable media and removable media devices to be compromised in any way whilst in their care or under their control.

4.2 Users must ensure that the use of removable media is limited to those times when no other method of storage or transportation of data is available or suitable and remote access to the data is not possible.

4.3 Users must ensure that personal/sensitive data or data which if lost or disclosed to unauthorised persons would cause damage to the Authority is encrypted when being copied or transferred onto removable media.

4.4 Users must ensure that appropriate security is put in place when data is transferred using removable media. Transfer of personal/sensitive data or data which if lost or disclosed cause could damage to the Authority should only take place after approval by a line manager.

4.5 Users must ensure that access to Authority information assets is limited to Authority personnel and that all data will be stored securely to prevent unauthorised access by third parties (including members of the employee's family).

4.6 Users must ensure that up-to-date anti-virus software is in place on the machine from which the data is copied and the machine to which the data is to be transferred.

4.7 Users must ensure that only Authority-owned removable media and devices are used. No personal removable media or removable media device should be attached to any computer on the network and Authority data should not be stored on any removable media or device which is not owned by the Authority.

4.8 Users must ensure that removable media under their control is stored in an appropriately secure and safe environment that prevents physical damage or loss.

4.9 Users must ensure that under no circumstances will software be copied from one machine to another without the appropriate licence agreement, only authorised staff may install, or move software.

4.10 Users must adhere to the corporate Document Retention Policy when storing data on removable media.

4.11 Users should be aware that data which is only held on removable media is at much greater risk of loss or destruction than data on corporate fileservers which is routinely backed up. Removable media should, therefore, not be the only place where data is held. Copies of the data should remain on the source system or computer until the data is successfully transferred to another computer or system, however care should be taken that the correct version of the file is being used.

4.12 Users should ensure that adequate version control is carried out and that old files are deleted when they are no longer required.

4.13 Users must ensure that when they leave the employment of the Authority or change post within the Authority any removable media associated with the post is returned to their line manager or HR. The removable media should be returned as it is i.e. not reformatted or wiped but the line manager should be informed if any of the data is sensitive or confidential. Any passwords associated with the media should be supplied to enable access to the documents. It should be noted that all data on Authority removable media is the property of the Authority. The unauthorised copying of Authority data is not allowed and could constitute a criminal offence.

4.14 Advice and guidance is available from the IT Service Desk or Business Relations Manager.

5. INCIDENT REPORTING

5.1 Any member of staff with concerns over the usage of removable media or a removable media device should bring the matter to the attention of line management, IT Service Desk or Business Relations Manager.

5.2 Loss or theft of removable media or device should be reported to a line manager, IT Service Desk or Business Relations Manager in accordance with the Incident Reporting Policy.

6. DISCIPLINARY CONSIDERATIONS

6.1 Misuse of removable media and removable media devices, information and software is considered a very serious matter. Disciplinary action will, when appropriate, be taken against employees who contravene this policy and this

could, in certain circumstances, lead to dismissal. Furthermore, misuse of computer programs or data, including unauthorised access to data, could lead to prosecution under the *Computer Misuse Act 1990*, *Copyright, Designs and Patents Act 1988* or the *Data Protection Act*.

7. GENERAL QUERIES

7.1 Any questions regarding this policy or computer security in general should be addressed to Steve John, the Head of ICT, on ext. 6218 or Ian John, Business Relations Manager, on ext 6036.