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

Mobile Device Security Policy

Version Control		
Version	**Date**	**Comments**
Version 1	May 2008	Initial draft of policy
	June 2009	Agreed with Unions
Version 1.1	Jan 2012	Review – small amendments and contact updates
Version 1.2	June 2013	Review & small amendments
Version 1.3	October 2014	Review & small amendments
Version 1.4	January 2016	Review & small amendments
Version 1.5	June 2017	Review & small amendments
Version 1.6	May 2018	Review & small amendments

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

MOBILE DEVICE SECURITY POLICY

1. INTRODUCTION

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

1.2. Mobile Device is a term used to define a host of different types of computer hardware, e.g.:

- Laptops/Notebooks/Netbooks
- Tablets/iPads
- PDA's
- Blackberries
- Mobile Telephones
- USB Flash Drives
- Digital cameras

1.3. In view of the Authority's reliance on information systems, these devices can be very beneficial to the authority and its workforce. They allow information to be available remotely, enable flexible working and whilst on the move, they can allow, for example, employees to visit service users at home and have access to relevant information. They also pose a very real threat to information security however, it would be counterproductive to ban or reduce the use of these devices, instead it is essential that the use and control of these devices is assessed and managed on risk. It must be remembered that the confidentiality, security and accurate processing of data (integrity) are of enormous importance.

2. RISK ASSESSMENT

2.1 Prior to approval being given to the purchase of a mobile device, a risk assessment should be carried out to determine the fitness for purpose of the device being contemplated. Often a portable device is considered appropriate when a more secure solution should be used. For example, a laptop purchased for use in an office environment with no intention of the machine being taken offsite.

2.2 Consideration should be given to the type of data which will be stored on the device which is to be purchased. If the data which is to be held on the device is sensitive then consideration must be given to security of that data. If after a risk assessment, it is decided that a mobile device is to be used for storage of sensitive data then the use of encryption must be considered and/or utilisation of a secure connection to the authority's network to access the information i.e. the data will not be stored on the portable device.

2.3 It should be acknowledged that the greatest risk is almost certainly the unauthorised disclosure of information rather than the value of the lost device which held the data.

2.4 The key risks are:

- The disclosure of sensitive information which is stored on mobile devices by loss of the device or by the information being seen or used by an unauthorised person
- Loss of information contained on mobile devices which could mean a disruption to the service.
- The cost of loss or damage to the equipment which could result from theft, misuse or carelessness by the user.
- The introduction of malware, viruses, etc to the network if devices become infected.
- Increased support costs for rectifying damage or tracing faults.

2.5 The risks are unlikely to be totally eliminated but can be mitigated through compliance with this policy.

2.6 Information and advice is available from the IT Service Desk or the Business Relations Manager.

3. MANAGERS RESPONSIBILITIES

3.1 Managers must ensure that an inventory of all mobile devices is in existence and shows:

- the person to whom the device has been allocated
- device description sufficient to identify the device i.e. the serial number, make and model
- date of purchase
- asset number

- other identifying numbers

3.2 Managers must ensure that the use of the mobile device has been risk assessed and that the data to be held upon the device is commensurate with security employed.

3.3 Managers should ensure that adequate security is in place when the mobile device is not in the office.

3.4 Managers should ensure that when employees terminate employment or transfer posts all mobile devices are returned in working order within an agreed timescale.

4. USERS RESPONSIBILITIES

4.1 It is the responsibility of all users to comply with this Policy. Each user must, therefore, ensure that they are familiar with its content

4.2 Users of mobile devices must ensure that they have sufficient competency in the use of the portable media device allocated to them.

4.3 Users are responsible for assigned mobile devices and the information contained upon them and must ensure that good care is taken of the device and the information is adequately protected. Mobile devices and the data held upon them are valuable assets and must be treated as such.

4.4 When users leave the authority any device issued to them must be returned in working order within an agreed timescale.

5. GUIDANCE FOR USE

5.1 To avoid loss or damage to the mobile device:

- Equipment should not be left unattended in plain view within reach of passers-by
- Security tags should not be removed from devices
- Mobile devices should be securely locked away when not in use even within the office e.g. overnight or when left unattended where the machine could be exposed to an opportunist thief.
- Laptops and other relevant mobile devices which are used in public areas should be secured with a security cable to guard against opportunist theft.

- Equipment should be stored securely out of sight whilst in transit e.g. in the boot of a car but should not be left in the car unattended e.g. overnight
- Mobile devices should not be transported whilst not in a carrying case due to the risk of damage
- Whilst away from the office employees should keep mobile devices with them
- Food, drinks and liquids should be kept away from the mobile device

5.2 To protect information held on or accessible by the mobile device ensure that:

- Mobile devices must never be used by or loaned to unauthorised persons
- Information held on or accessible by a mobile device should never be shown to unauthorised persons
- Where sensitive data is held on the mobile device a risk assessment should be carried out and where felt necessary encryption should be used
- No information is to be stored in or on any manual/paper records, computer system or software which is not owned by the Authority.
- Where the mobile device is to be used to access the Internet/e-mail a personal firewall should, if possible, be installed on the machine. Where a personal firewall is installed, the firewall must not be turned off.
- Where possible password access should be enabled
- Ensure that files and information are backed up regularly preferably to a network storage device/server.
- Access tokens (key fobs) which are used with the mobile device to access the authority's network should not be carried in the same bag as the mobile device.
- Anti virus software installed on the mobile device should not be tampered with as virus infections are often introduced by mobile devices which infect the network when reconnected. Where anti-virus software is installed on the device, the device must be connected to the authority network at least once per week for a minimum of one hour to keep the protection up-to-date.
- Ensure that the minimum of confidential information is held on the mobile device. Ensure that the data is limited to what is required for the current task. Any data held is at risk of loss, theft, damage or misuse.
- Ensure that when the device is in use in a public place confidential documents are not visible to others
- Mobile devices should not be connected to non-authority networks unless authorised
- If a mobile device is stolen, the police and IT Service Desk should be notified immediately. Details of the information stored on the device should also be provided.

5.3 To protect the Authority network:

- Unauthorised software must not be installed onto a mobile device
- Software must only be installed by authorised officers
- Unauthorised hardware i.e. equipment not owned by the Authority must never be connected to an Authority computer or network device. This includes laptops, PDAs, USB memory sticks/flash memory, mp3 players, cameras (including memory cards), etc.
- Authority owned mobile devices should not be used for personal purposes and should not be attached to the Internet at home unless specifically authorised.

6. MONITORING

6.1 Requests can be made for the return of a mobile device at any time to facilitate the auditing of the usage of the device. The device must be returned immediately or as agreed.

6.2 Use of unauthorised devices will be detected by authority systems.

7. INCIDENT REPORTING

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

8. HEALTH AND SAFETY

8.1 Exact Health and Safety procedure will vary from device to device, but some general guidance is found in the Authority's *Corporate Policy in respect of Display Screen Equipment*, the *Home Working Scheme* Document and appendices and in the Authority's *Health & Safety Booklet*, copies of which are available on the Authority's Intranet. Please contact the Corporate Health & Safety manager for further information.

9. DISCIPLINARY CONSIDERATIONS

9.1 Misuse of mobile 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* or the *Data Protection Act*.

10. GENERAL QUERIES

10.1 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.