



Great Yarmouth Borough Council Removable Media Policy

Author	Geoff Jones
Date	17 March 2009
Version	2.2
Last Review Date	2 March 2011
Review Changes	Added no data to be stored on Hard Disks
Document Status	Final

1.0 INTRODUCTION	3
1.1 POLICY RATIONALE	3
1.2 SCOPE	3
1.3 PRINCIPLES	3
2.0 REMOVABLE MEDIA POLICY.	4
2.1 REQUIREMENTS	4
2.2 ENFORCEMENT	4
2.3 PHYSICAL PROTECTION OF MOBILE EQUIPMENT	5
2.4 ACCESS CONTROLS	5
2.5 BACKUPS	5
2.6 VIRUS PROTECTION	5
2.7 USE OF THE FACILITIES IN PUBLIC PLACES	6
3.0 IMPLEMENTATION AND COMPLIANCE	6
3.1 IMPLEMENTATION	6
3.2 COMPLIANCE	6
4.0 EQUALITY IMPACT ASSESSMENT	7
5.0 HEALTH AND SAFETY	7
6.0 REFERENCE DOCUMENTS	7
7.0 DISTRIBUTION	7
8.0 REVIEW	7

1.0 INTRODUCTION

This policy forms part of the suite of policies dealing with data security.

The use of IT equipment by staff from Great Yarmouth Borough Council is an essential business requirement to keep in step with the demands for the retrieving, collating and communicating of information, in a fast, economic and secure manner.

The aim of this removable media policy is reduce the risk to the integrity and reputation of Great Yarmouth Borough Council, while maximising the use of these important business tools.

1.1 POLICY RATIONALE

At the time of the writing of this removable media policy in 2009, the council was aiming to meet the requirements to obtain and use a government connect secure circuit.

In 2009, the Council was of the view that there was a need to ensure that an agreed standardised approach was being taken to using removable media, in order to protect Council assets, and to ensure compliance with audit requirements.

This policy seeks to establish a standard set of conditions, and a framework for using removable media within the Council.

1.2 SCOPE

This Policy will apply to all Council employees who are required to use removable media to assist them in the performance of their duties.

1.3 PRINCIPLES

The Policy is designed to ensure that there are clear internal arrangements for the effective management of the use of removable media.

2.0 REMOVABLE MEDIA POLICY.

2.1 REQUIREMENTS

The first requirement is to determine whether you need to copy data onto removable media.

As a general rule you should not need to use removable media.

If you are travelling on council business is it really necessary to be able to connect to the council's network. If it is then connections via the CITRIX servers can be arranged, in this way the data does not leave the councils network.

2.2 ENFORCEMENT

Access to some information will be blocked.

If you prove via a business case that you have a genuine need to use removable media, then the data copied to the media will automatically be encrypted.

The following list is not exhaustive but indicates the types of equipment covered by this policy:

- Laptops/tablets/notebooks
- Personal Digital Assistant (PDA) e.g. Blackberry, Smartphone
- Mobile phones
- USB devices and media including Memory sticks, iPods, MP3 players, digital cameras, external/portable hard drives

Users must not install any personal software on the equipment

Users must not change the configuration of the equipment. Users must not attempt to connect the equipment to other private organisation's networks

The following rules will apply:

- Laptops, tablets and notebooks must be encrypted
- PDAs, mobile and smart phones that have Outlook Web Access installed or are used to store 'personal' or 'sensitive' information must have user access protected by PINs
- **Senior management must authorise the holding of 'personal' and 'sensitive' data on any portable equipment/devices/media and must maintain a log of such authorisations for audit purposes. Failure to comply with this policy is likely to result in disciplinary action.**
- CDs, DVDs and Laptop / Computer Hard drives must not be used to store 'personal' information or 'sensitive' Information.
- If 'personal' or 'sensitive' information needs to be held this may only be done on a Council supplied encrypted USB memory stick

2.3 PHYSICAL PROTECTION OF MOBILE EQUIPMENT

Mobile equipment must not be left unattended in insecure areas.

Locking devices, Kensington Locks, are issued as standard with all laptops. These must be used to attach the laptop to the fabric of the building.

Equipment must be stored out of view in a locked place.

In the event of loss inform the Service Desk as soon as possible

2.4 ACCESS CONTROLS

In addition to the specific controls above, PIN access codes must be enabled on all devices that offer the functionality.

2.5 BACKUPS

Information must be transferred to appropriate permanent network storage as a minimum on a daily basis.

2.6 VIRUS PROTECTION

Where virus protection is installed (for example Laptops) the equipment must be connected to the Council's network at least once a week for a minimum of one hour to keep the protection up to date. However, when uploads are large,

Infrastructure will make special arrangements.

These may include, for example bringing equipment into an office and connecting to the network or running a CD.

Equipment must only be connected to the network using approved methods.

If the equipment has not been connected to the network for 2 months, contact the service desk before connecting.

Users must not connect privately owned mobile devices or removable media such as cameras, iPods and phones to Council ICT equipment.

2.7 USE OF THE FACILITIES IN PUBLIC PLACES

Users should be wary of unauthorised people overlooking screens.

Users must be careful conveying sensitive information in public places.

Users must not leave their equipment unattended.

3.0 IMPLEMENTATION AND COMPLIANCE

3.1 IMPLEMENTATION

This policy will initially be implemented through the Chief Executive and Corporate Directors of the Council.

A memo will be sent to all HOD's and SUM's to make them aware of the policy.

It is the responsibility of managers to ensure that new staff receive information about this Policy, and should be part of any local induction where appropriate. Human Resources will add the Policy to its list of policy issues provided to any new starters. Managers must also ensure that any changes to this policy are effectively communicated within their areas of responsibility.

3.2 COMPLIANCE

Managers are responsible for ensuring that staff are aware of the location of this policy. In addition, Managers are responsible for keeping staff up to date about any changes within the policy.

All staff that are designated to use removable media are obliged to adhere to this Policy.

4.0 EQUALITY IMPACT ASSESSMENT

An equality impact assessment has been undertaken for the suite of policies relating to data security.

The result of this assessment shows low relevance in relation to specific equality issues and factors.

The full assessment can be found at:

<I:\Equality & Diversity\EIA\Equality Impact Assessments\Gov Connect\data security EIA.doc>

5.0 HEALTH AND SAFETY

There are no health and safety implications with this policy.

6.0 REFERENCE DOCUMENTS

This Policy should be read in conjunction with the following legislation, regulations and Council policies:

- COCO security checks
- Data Handling and Security Breaches
- System Access and Passwords
- Internet Security
- Email Usage
- IT Security
- Contractors / Suppliers connecting to the GYBC network
- Taking GYBC computer equipment abroad

7.0 DISTRIBUTION

This Policy will be available for all the Council's designated locations. Copies will also be available from the 'I' drive and on the Council's Intranet.

8.0 REVIEW

This Policy will be reviewed on an annual basis with the next review date being April 2012.