



Great Yarmouth Borough Council Taking Equipment Abroad Policy

Author	Geoff Jones
Date	17 March 2009
Version	2.1
Last Review Date	2 March 2011
Review Changes	None
Document Status	Final

1.0 INTRODUCTION	3
1.1 POLICY RATIONALE	3
1.2 SCOPE	3
1.3 PRINCIPLES	3
2.0 TAKING EQUIPMENT ABROAD POLICY	4
2.1 REQUIREMENTS	4
2.2 ENFORCEMENT	4
3.0 IMPLEMENTATION AND COMPLIANCE	5
3.1 IMPLEMENTATION	5
3.2 COMPLIANCE	5
4.0 EQUALITY IMPACT ASSESSMENT	5
5.0 HEALTH AND SAFETY	5
6.0 REFERENCE DOCUMENTS	6
7.0 DISTRIBUTION	6
8.0 REVIEW	6

1.0 INTRODUCTION

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

The use of IT networks 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 taking equipment abroad 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 taking equipment abroad 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 taking equipment abroad, 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 taking equipment abroad within the Council.

1.2 SCOPE

This Policy will apply to all Council employees who are required to take equipment abroad 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 taking equipment abroad.

2.0 TAKING EQUIPMENT ABROAD POLICY

2.1 REQUIREMENTS

The first requirement is to determine whether you need to take the equipment abroad.

If you are going on leave you do not need to take your laptop with you. Leave is part of your contract designed to create a total break from work, thus returning you able to perform to the required standard.

If you are travelling on council business is it really necessary to be able to connect to the council's network from your laptop. Would an internet café be suitable?

2.2 ENFORCEMENT

Access to some information will be blocked.

You will be able to access your standard emails from any internet café or internet hotspot but you will not be able to access emails in the secured system or access applications via the CITRIX server.

Before any equipment is taken out of the country permission must be granted by the Head of IT. Part of this permission will require your line manager to confirm that for this trip using council equipment abroad is a requirement of your job.

All service patches and antivirus software must be up to date. This must be confirmed by the support desk; they will check the revisions loaded.

If data is stored on the PC for the duration of the trip it must be encrypted.

Access to the equipment will be protected by local passwords.

Equipment must only be connected to other networks, hotspots, for the minimum time required to complete official use and tasks.

Upon your return the equipment needs to be checked again to ensure that any antivirus or patch updates are applied.

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 as able to take equipment abroad 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
- Using Removable Media
- Contractors / Suppliers connecting to the GYBC network

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.