



Great Yarmouth Borough Council
Removing Disabled IT Accounts Policy

Author	Geoff Jones
Date	23 February 2010
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 DELETING DISABLED IT ACCOUNTS POLICY	4
2.1 REQUIREMENTS	4
2.2 ENFORCEMENT	4
3.0 IMPLEMENTATION AND COMPLIANCE	4
3.1 IMPLEMENTATION	4
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 deleting disabled IT accounts 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 deleting disabled IT accounts policy in 2010, the council required clarification of the actions to be taken when a member of staff left to meet the recommendations in the IT audit report.

This policy seeks to establish a standard set of conditions, and a framework for deleting disabled IT accounts within the Council.

1.2 SCOPE

This Policy will apply to all Council employees and will be used by ITSS to ensure the security of the councils network.

1.3 PRINCIPLES

The Policy is designed to ensure that there are clear internal arrangements for the effective management of deleting disabled IT accounts.

2.0 DELETING DISABLED IT ACCOUNTS POLICY

2.1 REQUIREMENTS

Notification that a member of staff is leaving will be supplied to ITSS by HR, this will give the leaving date.

ITSS will log an action to suspend the account at the end of the last working day.

The member of staff concerned will be sent a reminder from ITSS to delete or transfer any information in their 'U' drive to their manager.

At close of business on the day the member of staff leaves their account will be suspended.

Within 5 working days the user ID will be deleted along with any remaining contents of the 'U' drive.

In exceptional circumstances the member of staff's manager can request the temporary diversion of incoming external emails to another account; this will be set up as a rule on the server for a maximum of 2 Months along with a message to the sender informing them that the account has been closed. This diversion must have the agreement of the ITSS manager.

Copies of data originally on the 'U' drive will then be automatically deleted as the current cycle of saves rotates.

2.2 ENFORCEMENT

This policy will be enforced by the ITSS section and will automatically be activated on the resignation of a member of staff.

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.

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
- Taking 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.