



Great Yarmouth Borough Council COCO Security Checks 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 COCO SECURITY CHECKS POLICY.....	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 and systems within 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 the coco security checks policy is to allow the authority to comply with the requirements for connecting to the GovConnect network for the transfer of information between registered public bodies.

1.1 POLICY RATIONALE

At the time of the writing of this COCO Security Checks 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 the COCO Security Checks, 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 the COCO Security Checks within the Council.

1.2 SCOPE

This Policy will apply to all Council employees who are required to view or receive data that has been classed as restricted or above 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 COCO Security Checks.

2.0 COCO SECURITY CHECKS POLICY.

The Baseline Personnel Security Standard (BPSS) is fully documented in HMG Standard that is obtainable from the I Drive, but is detailed below for convenience.

There is no requirement for a CRB check to be applied for BPSS, only a personal declaration.

A BPSS check involves checking:

1) Proof of identity, by visibility of:

- Full 10 year passport

Or two from the below list:

- British driving license
- Form P45
- Birth Certificate
- Proof of residence i.e. council tax or utility bill

2) Employment history (past 3 years)

3) Nationality and immigration status

4) Criminal Record Declaration (unspent convictions only)

To ensure compliance with this policy a record of these checks being done will be supplied by the employing department this acknowledgement will be stored on the user record in the support desk system before access is granted to GCSX.

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 receiving restricted information 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:

- 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 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.