



**Great Yarmouth Borough Council**  
**Contractors / Suppliers connecting to Great**  
**Yarmouth Borough Councils Network Policy**

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

<b>1.0 INTRODUCTION</b> .....	3
<b>1.1 POLICY RATIONALE</b> .....	3
<b>1.2 SCOPE</b> .....	3
<b>1.3 PRINCIPLES</b> .....	3
<b>2.0 CONTRACTORS / SUPPLIERS CONNECTING TO GREAT YARMOUTH BOROUGH COUNCILS NETWORK POLICY</b> .....	4
<b>2.1 REMOTE CONNECTIVITY</b> .....	4
<b>2.2 SECURITY CHECKS</b> .....	4
<b>2.3 DATA ACCESS AND TRANSFER</b> .....	5
<b>3.0 IMPLEMENTATION AND COMPLIANCE</b> .....	6
<b>3.1 IMPLEMENTATION</b> .....	6
<b>3.2 COMPLIANCE</b> .....	6
<b>4.0 EQUALITY IMPACT ASSESSMENT</b> .....	8
<b>5.0 HEALTH AND SAFETY</b> .....	8
<b>6.0 REFERENCE DOCUMENTS</b> .....	8
<b>7.0 DISTRIBUTION</b> .....	8
<b>8.0 REVIEW</b> .....	8

## **1.0 INTRODUCTION**

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

The use of contractors and the support from suppliers for their systems is essential for Great Yarmouth Borough Council to keep the systems up to date so as 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 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 and to allow the contractors / suppliers to continue to provide support to the systems we are running.

## **1.1 POLICY RATIONALE**

At the time of the writing of this Contractors / Suppliers connecting to Great Yarmouth Borough Councils Network 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 Contractors / Suppliers connecting to Great Yarmouth Borough Councils Network, 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 Contractors / Suppliers connecting to Great Yarmouth Borough Councils Network.

## **1.2 SCOPE**

This Policy will apply to all Contractors / Suppliers connecting to Great Yarmouth Borough Councils Network.

## **1.3 PRINCIPLES**

The Policy is designed to ensure that there are clear internal arrangements for the effective management of Contractors / Suppliers connecting to Great Yarmouth Borough Councils Network.

## **2.0 CONTRACTORS / SUPPLIERS CONNECTING TO GREAT YARMOUTH BOROUGH COUNCILS NETWORK POLICY.**

### **2.1 REMOTE CONNECTIVITY.**

Any remote connections will be authenticated using dual factor authentication.

Companies that support systems will only have access to the servers hosting the applications they supply. They will, if required, be granted local admin rights to the server(s) hosting the applications but they will not have domain admin rights.

Access to the Council's network for third party support will be restricted to when fault calls are raised or access is requested by the supplier. Unless requested by the supplier, links will be terminated outside of business or agreed support hours as documented in their SLA. All fault calls and requests for access must be via the GYBC Support Desk.

### **2.2 SECURITY CHECKS.**

Support staff must be vetted to the base line security standard.

The Baseline Personnel Security Standard (BPSS) is fully documented in HMG Standard, 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)

### **2.3 DATA ACCESS AND TRANSFER**

Support staff must also be aware of their responsibilities regarding access to data specifically with reference to the data protection act.

If it is necessary for data to be transferred to the supplier wherever possible personal information must be replaced with dummy records. If real data is transferred then the time it is kept, its location and the method of disposal must be agreed and this agreement must comply with current COCO policies.

An audit trail of all connections, work carried out, data transferred and its final disposal will be kept.

### **3.0 IMPLEMENTATION AND COMPLIANCE**

#### **3.1 IMPLEMENTATION**

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

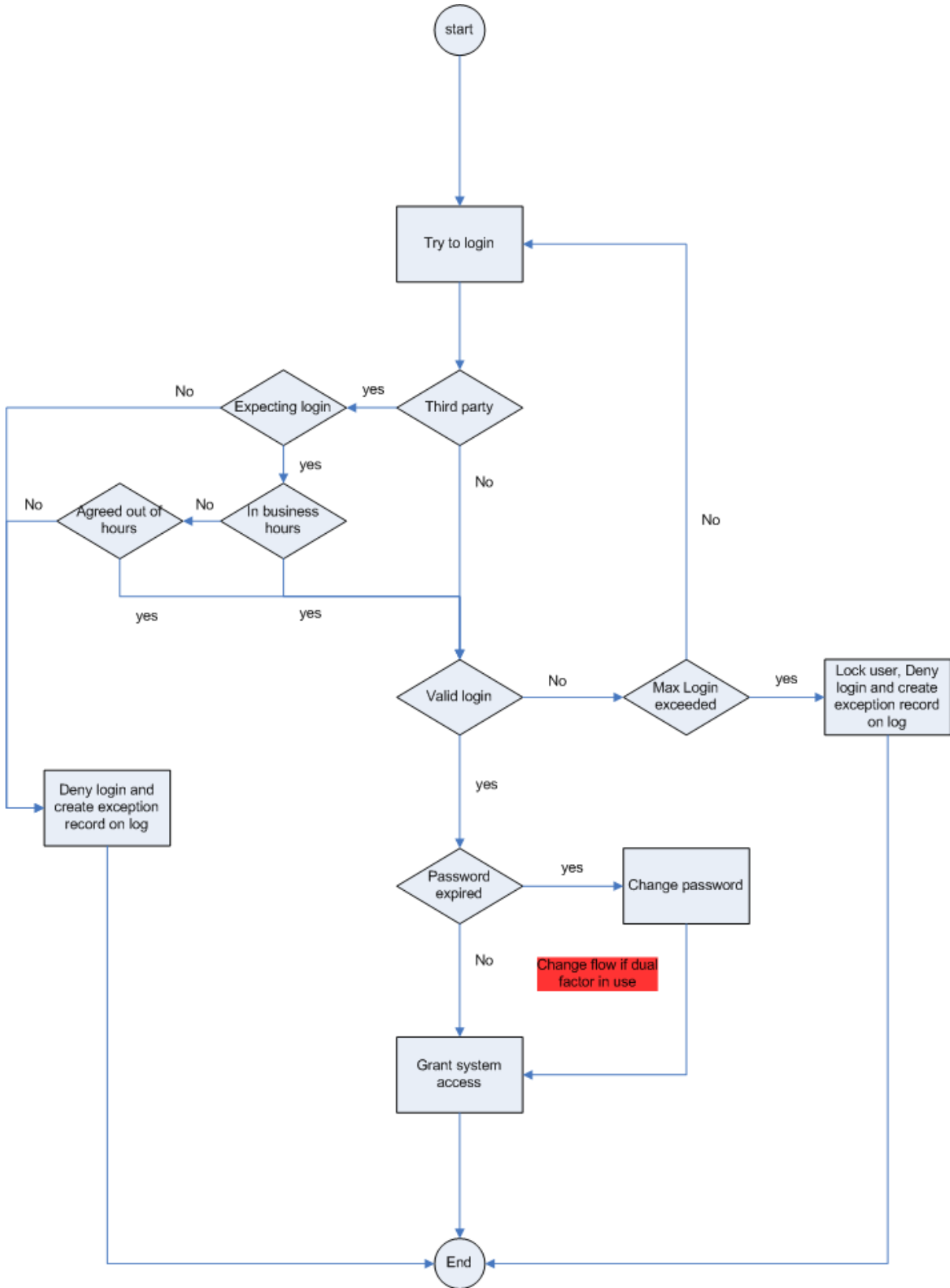
A memo will be sent to all HOD's and SUM's to make them aware of the policy.

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.

The following flow diagram will be used to ensure that contractors / suppliers connecting to Great Yarmouth Borough Councils network 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
- 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.