



## Great Yarmouth Borough Council Internet Security Policy

Author	Geoff Jones
Date	17 March 2009
Version	2.1
Last Review Date	2 March 2011
Review Changes	Removed references to payroll deductions
Document Status	Final

<b>1.0 INTRODUCTION</b> .....	3
<b>1.1 POLICY RATIONALE</b> .....	3
<b>1.2 SCOPE</b> .....	4
<b>1.3 PRINCIPLES</b> .....	4
<b>2.0 EMAIL USAGE POLICY</b> .....	5
<b>2.1 RISKS INVOLVED WITH USING THE INTERNET</b> .....	5
<b>2.2 AUTHORISED USE</b> .....	5
<b>2.3 PRIVATE INTERNET USE</b> .....	6
<b>2.4 SECURITY</b> .....	6
<b>2.5 NON-ACCEPTABLE BEHAVIOUR</b> .....	7
<b>2.6 INTERNET BROWSING</b> .....	8
<b>2.7 FILE TRANSFER PROTOCOL (FTP)</b> .....	9
<b>2.8 REMOTE ACCESS (TELNET)</b> .....	9
<b>2.9 SUMMARY &amp; DECLARATION</b> .....	10
<b>3.0 IMPLEMENTATION AND COMPLIANCE</b> .....	11
<b>3.1 IMPLEMENTATION</b> .....	11
<b>3.2 COMPLIANCE</b> .....	11
<b>4.0 EQUALITY IMPACT ASSESSMENT</b> .....	11
<b>5.0 HEALTH AND SAFETY</b> .....	11
<b>6.0 REFERENCE DOCUMENTS</b> .....	12
<b>7.0 DISTRIBUTION</b> .....	12
<b>8.0 REVIEW</b> .....	12
<b>Declaration</b> .....	13
<b>Payroll Deduction.</b> .....	<b>Error! Bookmark not defined.</b>

## 1.0 INTRODUCTION

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

The use of developing technology within Great Yarmouth Borough Council is an essential business requirement to keep in step with the demands for the retrieving, collating and communication of information, in a fast, economic and secure manner. The expansion of the Internet and the application of Internet Services, provide a growing range of tools which benefit the operation of an authority and its interaction with the community.

The aim of this Internet Security Policy is to reduce the risk to the integrity of the resources and reputation of Great Yarmouth Borough Council, while maximising the use of Internet based technology as an important business tool.

## 1.1 POLICY RATIONALE

At the time of the writing of this Internet Security 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 Internet Security, 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 Internet Security within the Council.

The Internet provides services with a global reach, extending to Great Yarmouth Borough Council the amount of information available and the ability to make information available to other agencies, businesses and the general public. To this extent the use of these resources could have a significant impact well beyond the boundaries of our authority i.e. worldwide.

The policies set out in this document are intended to address Internet security concerns and to protect the name and reputation of Great Yarmouth Borough Council.

The computer systems of Great Yarmouth Borough Council and the confidential information contained upon them are an **essential resource** and require **adequate protection**.

Failure by **any user** to adhere to these policies or any other misuse of the Internet resources may result in **disciplinary action**.

**Misuse of Great Yarmouth Borough Council Internet resources could have serious consequences including, but not limited to dismissal, criminal prosecution or civil liability.**

## **1.2 SCOPE**

This Policy will apply to all Council employees.

## **1.3 PRINCIPLES**

The Policy is designed to ensure that there are clear internal arrangements for the effective management of Internet Security.

## 2.0 EMAIL USAGE POLICY

### 2.1 RISKS INVOLVED WITH USING THE INTERNET

The use of any Internet services brings with it certain risks. The improper use of Internet services can have an adverse effect on the name and reputation of Great Yarmouth Borough Council.

Much of the information and software available via the Internet is provided without any warranty as to its accuracy, legal status, or that it will work in a prescribed manner. In this respect information obtained via the Internet may appear as fact, but be either incorrect, a personal opinion or out of date.

To this extent, the validity and accuracy of any such information should be verified by another means before being used or referenced. In addition information obtained from the Internet may infringe the intellectual property rights of a third party, despite there not being any explicit warning.

Software may include viruses, destructive elements or other detrimental aspects. Nor may the software operate in an intended manner or be compatible with a particular system, which may in itself lead to technical problems and the loss of data.

### 2.2 AUTHORISED USE

- Great Yarmouth Borough Council Internet resources must only be accessed and used for the purposes of Great Yarmouth Borough Council business, unless the user has opted to accept the Authority's concession for private use.
- All users must have signed the 'declaration' at the end of this document stating that they have read, understood and agreed to follow the terms and conditions set out in the Internet Security Policy.
- The public Internet should not be used for transaction processing, contracts, or as a substitute for Great Yarmouth Borough Council's own electronic mail. Care should be taken to avoid making any statements that may be interpreted as contractual. **(This should not be confused with e-commerce done on a secure server.)**
- The Internet must not be used for confidential/sensitive business communications unless such information is protected by an appropriate security mechanism. In such cases, only security mechanisms approved by Great Yarmouth Borough Council may be used in securing communications.

- Use of any external resources that are accessed through Great Yarmouth Borough Council's Internet connection must be in a manner consistent with the policies and guidelines of the owners of those resources.
- Establishing unauthorised network connections between Great Yarmouth Borough Council and any other network is prohibited.
- Use of Internet Gateways (including modem connections) other than Great Yarmouth Borough Council's Internet Gateway is prohibited. Attempts to bypass Great Yarmouth Borough Council's Internet Gateway will result in disciplinary actions.
- System security measures (such as virus checkers and browser security) have been specifically installed in order to protect the integrity of the authority's resources and the information contained upon them.
- Users shall at no point deactivate nor alter the level of security within software nor change the security settings of IT equipment.

### **2.3 PRIVATE INTERNET USE**

- It has been decided that members of staff may make private use of the Authority's Internet facilities, provided it is done in their **OWN TIME**.
- Whilst using the facilities for private use staff members will be bound by the same conditions applying to official use

### **2.4 SECURITY**

- Passwords are the personal responsibility of each user. Passwords should at all times be kept private and secure and changed at least every **Thirty DAYS AND BE COMPLEX**. Passwords should not be written down nor shared with any other party.
- If you have reason to believe that the security of your password has been compromised you should inform the **Integrated Technical Support Services** (ITSS) department immediately and change your password.
- Users are prohibited from installing any software obtained from the Internet on either personal computers or on any Great Yarmouth Borough Council network. (Programs may be automatically downloaded by some technical sites - these can normally be ignored. If concerned contact the **Integrated Technical Support Services** department support desk on 846333 or email [servicecdesk@great-yarmouth.gov.uk](mailto:servicecdesk@great-yarmouth.gov.uk))

To obtain such software or software upgrades, a request should be made to the **Integrated Technical Support Services** department. This is required because downloaded software must be inspected for computer code that may disrupt, disable, harm or otherwise impede the operation of the computer system or network. Furthermore such software may require appropriate licensing before it can be used within Great Yarmouth Borough Council, it must be noted that such software may only be allowed for Personal Use and NOT Business use. There is also the question of copyright and Intellectual Property considerations. Copying anything from the internet such as wallpaper could be illegal.

Users must also be aware of the security implications when using Laptops. Permission should always be sought if a User has a GY Borough Council Laptop and wants to use this at home then they must check with ITSS Dept before doing so. Contracted home workers will always use a GYBC supplied business line. No equipment except that supplied by GYBC is allowed to be connected to the GYBC internal network.

Users have all their Internet activities monitored and recorded and should have no expectation of privacy for any Internet use unless national law, regulation or contract provides otherwise.

Users are specifically advised that their use of the Internet indicates their consent to this monitoring and to all appropriate disclosure of any evidence of criminal activity or violation of Great Yarmouth Borough Council's rules, policies, procedures or standards of conduct.

ALL USERS ARE RESPONSIBLE FOR INFORMING THE **INTEGRATED TECHNICAL SUPPORT SERVICES** DEPARTMENT IF THERE IS ACTUAL OR POTENTIAL VARIATION FROM THE POLICIES SET OUT IN THIS DOCUMENT.

## **2.5 NON-ACCEPTABLE BEHAVIOUR**

- Users must not retrieve or download any information or material that may be considered offensive, abusive, racist, sexist or discriminatory.

Examples of behaviour that may result in disciplinary action follow (please note that this list is not exhaustive and does not include all possible actions). Disciplinary actions can range from verbal warnings to dismissal. Whilst it has been agreed that users may make use of the Internet resources, in their own time, and may use it for personal communications the following must apply:

Users of Great Yarmouth Borough Council Internet resources must not use the resources:

- For soliciting personal gain, money or in the operation of a personal business;

- To gain unauthorised access to any computer system of Great Yarmouth Borough Council, or any other organisation;
- To copy electronic files without permission;
- To send or transfer confidential materials belonging to Great Yarmouth Borough Council outside of Great Yarmouth Borough Council, or to transfer confidential materials of Great Yarmouth Borough Council to an unauthorised personnel within Great Yarmouth Borough Council.

## **2.6 INTERNET BROWSING**

The way in which information can be retrieved from the Internet is essentially a form of file transfer mechanism. As such, the file transfer guidelines contained in this document should be followed when using an Internet browser to access resources. Users should only use the licensed copies of approved software (e.g. Microsoft Internet Explorer) provided by Great Yarmouth Borough Council to access the Internet.

The speed at which information can be retrieved from the Internet will depend to a large extent on the number of concurrent users within the local Great Yarmouth Borough Council network. In order to maximise the effectiveness of the resources, users should try to use the time connected to the Internet constructively.

- Users should not change the browser proxy or security configuration. Any unauthorised changes will create problems for the network. (If in doubt do not amend any settings on software provided).
- Users are NOT allowed to access any Live Radio links online (streaming media). This is PROHIBITED due to the large bandwidth that is required to listen to it.
- Users are NOT allowed to access any 'FEEDS' that may be advertised i.e. BBC Ticker.

## **2.7 FILE TRANSFER PROTOCOL (FTP)**

FTP is a system by which computer files can be transferred from one server to another using an Internet connect. There are many services available on the Internet which allows computer files, such as software and documents, to be transferred from a remote site to the user's local computer.

Users must not transfer files to any computer system but should ask the ITSS Department to do so for them. Any such transfers must be authorised by the Departmental Manager.

Always be aware of the size of file that you are transferring and the likely impact that this may have on the Great Yarmouth Borough Council network.

## **2.8 REMOTE ACCESS (TELNET)**

Telnet is a method of logging into a server from a remote location using an Internet connection. A user is only allowed to remotely access servers with which the user has an authorised user account (a registered login), or to servers that advertise anonymous (guest) access.

**GREAT YARMOUTH BOROUGH COUNCIL PERSONNEL SHOULD OBSERVE ALL POSTED RESTRICTIONS AND PROHIBIT THE USE OF UNAUTHORISED PORTS.**

Exceptions to the above will be considered on a case by case basis and will be dependent on the duties of the officer requiring the variance to the general rules.

A business case supported by the head of department must be submitted to the IT manager

## 2.9 SUMMARY & DECLARATION

The Internet is a massive source of business information that may help increase the productivity of your day-to-day activities. As all users share a common pipeline to the Internet we need certain rules to keep performance at an acceptable level and keep our environment safe.

- Approach the Internet with caution and commonsense.
- Whilst permission is given for personal use of Internet access and email, in users own time, it should not be used for any commercial or business purposes other than those of Great Yarmouth Borough Council.
- Use virus scan for downloaded data from the Internet.
- The installation of downloaded or otherwise obtained applications and plug-ins is not allowed without the express permission of the ITSS department.
- Misuse of copyrighted material in our business activities is not allowed.
- The Internet is not to be used for personal and or confidential data.
- Whilst personal use of the internet is available long periods of Recreational surfing is not allowed, as this will 'tie-up' the facility possibly stopping other user from gaining access.
- Do not complete online surveys, unless the data is general information, the answers will not be secure.

### **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.

Service managers are responsible for ensuring that all employees and agents are trained in using the Internet resources and that they have read and signed this document, so that users are aware of the requirements of the Internet security policy.

All staff 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
- 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.

**Declaration**

I, \_\_\_\_\_, hereby confirm to have read and understood the Internet and Email Policy of the Great Yarmouth Borough Council and hereby formally confirm to abide by it at all times. I understand that any deviation from the policy will be reported to Management. I further understand that this policy covers personal use of these facilities.

Signature

Date:

This form is to be filed in the ITSS Dept.

.....