



Great Yarmouth Borough Council

Email Usage Policy

Author	Geoff Jones
Date	17 March 2009
Version	2.1
Last Review Date	2 March 2011
Review Changes	Statement on subject line impact level marking added
Document Status	Final

1.0 INTRODUCTION	3
1.1 POLICY RATIONALE	3
1.2 SCOPE	3
1.3 PRINCIPLES	4
2.0 EMAIL USAGE POLICY	5
2.1 RISKS INVOLVED WITH USING EMAIL	5
2.2 AUTHORISED USE:	5
2.3 NON-ACCEPTABLE BEHAVIOUR	6
2.4 GCSX EMAILS	8
2.5 SUMMARY & DECLARATION	9
3.0 IMPLEMENTATION AND COMPLIANCE	10
3.1 IMPLEMENTATION	10
3.2 COMPLIANCE	11
4.0 EQUALITY IMPACT ASSESSMENT	11
5.0 HEALTH AND SAFETY	11
6.0 REFERENCE DOCUMENTS	12
7.0 DISTRIBUTION	12
8.0 REVIEW	12

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 Email provides a growing range of tools which benefit the operation of an authority and its interaction with the community.

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

1.1 POLICY RATIONALE

At the time of the writing of this Email Usage 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 use of Email, 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 Email usage within the Council.

The policies set out in this document are intended to address Email Usage 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 Email resources may result in **disciplinary action**.

Misuse of Great Yarmouth Borough Council Email 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 Email usage.

2.0 EMAIL USAGE POLICY.

2.1 RISKS INVOLVED WITH USING EMAIL

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

Users should be aware that information transferred across the Internet could be intercepted, viewed, altered or destroyed by unauthorised individuals before reaching the intended recipient.

As with conventional mail there is also the risk that information may not arrive or may be unduly delayed.

Information that is transmitted via the Internet from Great Yarmouth Borough Council is likely to either contain the name Great Yarmouth Borough Council in the return address or details which will allow Great Yarmouth Borough Council to be identified as the sender. Once such information has been transmitted, either by electronic mail, online form or news service, it cannot be recalled.

Users should ensure that information to be sent is correct and is not likely to damage the name and reputation of Great Yarmouth Borough Council.

The use of Email provides Great Yarmouth Borough Council 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.

2.2 AUTHORISED USE:

- Great Yarmouth Borough Council Email resources must only be accessed and used for the purposes of Great Yarmouth Borough Council business.
- 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 Email Usage Policy.
- 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.)**

- Email 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.
- The name of Great Yarmouth Borough Council will appear automatically in the heading of a message or it will be possible for the recipient to identify Great Yarmouth Borough Council as the originator of the message by tracing the path of the message.
- System security measures (such as virus checkers) 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.

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

Users are specifically advised that their use of Email 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.

2.3 NON-ACCEPTABLE BEHAVIOUR

- Users must never send any material that is inflammatory, threatening, harassing (racially, sexually or otherwise), defamatory, disruptive to others' operations, or otherwise reflect poorly on the name and reputation of Great Yarmouth Borough Council using the Internet resources of Great Yarmouth Borough Council.
- Users must not retrieve or download any information or material that may be considered offensive, abusive, racist, sexist or discriminatory.

Examples of behavior 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 Email resources must not use the resources:

- For soliciting personal gain, money or in the operation of a personal business;
- To originate or distribute chain letters;
- To send racially, sexually or otherwise threatening or harassing messages;
- 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.
- The security of electronic mail that is sent via the Internet cannot be guaranteed.

When sending any information that uses the public Internet (such as application or request forms found on Internet web sites, bulletin boards and newsgroup postings), never include anything that you want to keep private and confidential.

Please remember that the guidelines for electronic mail apply to Internet mailing lists and other discussion forums.

Ensure that both you and the party you are communicating with understand all of the risks involved in using the Internet as a communication mechanism.

Users must include the council's standard signature as fully described in the council's customer care standards.

When users wish to ensure that email has been delivered, they should check by using a different way of communication. The sending of an electronic mail in the prescribed manner is no guarantee that it will arrive or that it will be delivered to the appropriate addressee.

Although many systems incorporate a receipt function, it is not a guarantee that people have received your message.

Users should also verify the sender of any electronic mail before relying on the

information contained, if the sender was unknown or the information not expected.

Any file or information which is received, as an email attachment using electronic mail, should be verified using the Great Yarmouth Borough Council authorised virus scanning software before being opened. (This will normally be picked up by the service provider that we use for email transmission). If unsure contact the ITSS Department.

The sending and receiving of large attachments can cause delays and technical problems for the whole electronic mail system. It may also result in the attachment being deleted automatically. Before sending or receiving large attachments, please check with the ITSS Department that it is safe to do so.

Users should also be aware that as a security precaution, the Great Yarmouth Borough Council firewall might not allow the delivery of certain types of attachment or messages. (A firewall is a hardware/software mechanism for preventing unauthorised access to the Internet resource).

The firewall may, in some circumstances, alter the layout or format of an attachment. Care should be taken to verify that the file or information you send or receive is delivered complete and in the intended format. Users concerned about ensuring that information arrives in the manner in which it was intended should first consult the ITSS department for advice.

2.4 GCSX EMAILS

GCSX emails are secure emails transmitted and received over a secure circuit. Due to the nature of the information potentially contained within these emails the handling of them is different.

Staff who receive these type of emails need to read and understand the policy on data handling and security breaches.

In essence there are a few simple rules to obey:

- GCSX emails can only be received via a dedicated GCSX email account.
- These emails cannot be received on blackberries or other remote devices.
- These emails cannot be forwarded to other email systems including the council's internal email system or hotmail accounts.
- If the information contained in these emails is subsequently stored on the councils data network or in hard copy form it must contain the appropriate security level markings.

- The subject line of these emails must contain their impact level marking.

2.5 SUMMARY & DECLARATION

The Email mail system is fast becoming one of the most important forms of communication within the authority. We currently ensure the delivery of over 4000 messages per day. In order to keep this form of communication as fast as possible the following guidelines are in force:

- The mail system facility is provided for **BUSINESS USE ONLY** (not for sending MP3s, screensavers, games, movies, etc.).
- Great Yarmouth Borough Council treats all messages sent, received or stored in the email system as business information.
- If you receive other content, please request the originator to stop sending this type of content immediately.
- The maximum message size is 10MB, any attachment greater than this please advice the ITSS Department who will take special measures to send it.
- Your messages will travel faster through the network if you use WinZip to package an attachment >100KB. The **Integrated Technical Support Services** department will assist users to do this.
- **Do not** use the authority mail system to send around joke or junk messages
- When sending an email you should consider that there is a possibility that the message may be misdirected or become public knowledge.
- When using Internet mail, it is impossible to ensure that the message actually reaches the recipient - there is no way to track the delivery process.
- Always use care in addressing email messages to make sure messages are not inadvertently sent to the wrong person. In particular, exercise care when using distribution lists - check that all addressees are appropriate recipients of the information.

- Great Yarmouth Borough Council confidential information should never be forwarded to non-Great Yarmouth Borough Council individuals or companies not authorized to receive that information.
- There is no way to be sure that the originator is the actual person who sent you the message.
- If you are unsure about an attachment, please consult the **Integrated Technical Support Department** before opening it - there may be a virus infection risk.
- The transmission of copyrighted or pornographic materials is forbidden at all times.
- Use Internet mailing lists in a sensible way - limit your number of subscriptions to those mailing lists for business use only.
- Take into account that the Internet is not a secure communications channel when you consider sending confidential documents.
- Email etiquette: refrain from routinely forwarding messages to multiple parties unless there is a clear business need to do so - take care to ensure that your messages are courteous, professional and business-like - write as if your email may be published in a newspaper or become part of a court case - use the standardized email signature/disclaimer as proposed.
- **Do not** participate in forwarding chain letters.
- **Do not** send or forward any defamatory, offensive or harassing messages.
- **Do** report any suspicious activities to the ITSS Service desk (846333).
- Please remember that any mail you send out will mention @great-yarmouth.gov.uk in the address line.

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 also responsible for ensuring that all employees and agents are trained in using the Email resources and that they have read and signed this document, so that users are aware of the requirements of the Email Usage 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:

- COCO security checks
- Data Handling and Security Breaches
- System Access and Passwords
- Internet Security
- 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.