

## Email Policy



*A great place to live, work & play*

**DOCUMENT CONTROL**

<b>Organisation</b>	Scarborough Borough Council
<b>Title</b>	Email Policy
<b>Author</b>	Andy Tolley
<b>Filename</b>	[Saved Filename]
<b>Owner</b>	ICT Manager
<b>Subject</b>	ICT Policy
<b>Protective Marking</b>	NOT PROTECTIVELY MARKED
<b>Review date</b>	April 2019

**Revision History**

<b>Revision Date</b>	<b>Reviser</b>	<b>Previous Version</b>	<b>Description of Revision</b>
June 09	Andy Tolley		Initial creation
July 09	ICT Services	0.1	Review by ICT Services
July 09	HR	0.2	Review by HR
July 09	ICT Services	0.3	Final
April 2019	Petra Jackson	0.4	Name Changes and post titles etc

**Contributors**

Development of this policy was assisted through information provided by West Midlands Local Government Association.



## Contents

1	Policy Statement	4
2	Purpose	4
3	Scope	4
4	Definition	4
5	Risks	5
6	Applying the Policy	5
6.1	Email as Records	5
6.2	Email as a Form of Communication	6
6.3	Junk Mail	8
6.4	Mail Box Size	8
6.5	Monitoring of Email Usage	8
6.6	Categorisation of Messages	9
6.7	Security	10
6.8	Confidentiality	10
6.9	Negligent Virus Transmission	11
7	Policy Compliance	11
8	Policy Governance	11
9	Review and Revision	12
10	References	12
11	Key Messages	13
	Appendix 1	14



## **1 Policy Statement**

Scarborough Borough Council will ensure all users of Council email facilities are aware of the acceptable use of such facilities.

## **2 Purpose**

The objective of this Policy is to direct all users of Council email facilities by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.
- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can apply self-regulation to their use of email as a communication and recording tool.

## **3 Scope**

This policy covers all email systems and facilities that are provided by Scarborough Borough Council for the purpose of conducting and supporting official business activity through the Council's network infrastructure and all stand alone and portable computer devices.

This policy is intended for all Scarborough Borough Council Councillors, Committees, Service Areas, Partners, Employees of the Council, contractual third parties and agents of the Council who have been designated as authorised users of email facilities.

The use of email facilities will be permitted only to staff that have been specifically designated as authorised users for that purpose, received appropriate training and have confirmed in writing that they accept and agree to abide by the terms of this policy.

The use of email facilities by staff that have not been authorised for that purpose will be regarded as a disciplinary offence.

## **4 Definition**

All email prepared and sent from Scarborough Borough Council email addresses or mailboxes, and any non-work email sent using Scarborough Borough Council ICT facilities is subject to this policy.



## 5 Risks

Scarborough Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Non-reporting of information security incidents
- Inadequate destruction of data
- Removal of data from the Councils infrastructure
- Loss of direct control of access to information systems and facilities

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy

### 6.1 Email as Records

All emails that are used to conduct or support official Scarborough Borough Council business must be sent using a “@Scarborough.gov.uk” address. All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format “@Scarborough.gcsx.gov.uk”.

Non-work email accounts **must not** be used to conduct or support official Scarborough Borough Council business. Councillors and users must ensure that any emails containing sensitive information must be sent from an official council email. Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email (please also refer to section 6.7). All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Emails held on Council equipment are considered to be part of the corporate record and email also provides a record of staff activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Scarborough Borough Council business should be considered to be an official communication from the Council. In order to ensure that Scarborough Borough Council is protected adequately from misuse of e-mail, the following controls will be exercised:

- i. It is a condition of acceptance of this policy that users comply with the instructions given during the email training sessions.
- ii. All official external e-mail must carry the following disclaimer:



*This email (and any files transmitted with it) may contain confidential or privileged information and is intended for the addressee only.*

*If you are not the intended recipient, please be aware that any disclosure, copying, distribution or any action taken is prohibited and may be unlawful - you should therefore return the email to the sender and delete it from your system.*

*Any opinions expressed are those of the author of the email, and do not necessarily reflect those of Scarborough Borough Council.*

*This email has been checked for the presence of computer viruses, but please rely on your own virus-checking procedures.*

Whilst respecting the privacy of authorised users, Scarborough Borough Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the Council's ICT systems.

It should also be noted that email and attachments may need to be disclosed under the GDPR/Data Protection Act or the Freedom of Information Act 2000. Further information regarding this can be obtained from the Council's Data Protection Officer and/or Freedom of Information Officer.

## **6.2 Email as a Form of Communication**

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or PROTECT or RESTRICTED information or of communicating in the particular circumstances.

All emails sent to conduct or support official Scarborough Borough Council business must comply with corporate communications standards. Scarborough Borough Council Email Usage Policy gives advice on acceptable/unacceptable content in email

Councillors must ensure that any emails containing sensitive information must be sent from an official council email. Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email.

Email must not be considered to be any less formal than memo's or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council's reputation or its relationship with customers, clients or business partners.



Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities Policy or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any material, should consult their line manager prior to commencing any associated activity or process.

ICT facilities provided by the Council for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of PROTECT or RESTRICTED material concerning the activities of the Council.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the Council into disrepute.



### 6.3 Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using Scarborough Borough Council systems or facilities.

### 6.4 Mail Box Size

In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addressees is discouraged.

Users will be provided with a limited mail box size during 2010 to reduce problems associated with server capacity. Email users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems. This policy must be read in conjunction with the Council's e-mail usage guidelines.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox

### 6.5 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic will be undertaken so that Scarborough Borough Council:

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.

Monitoring of content will only be undertaken by staff specifically authorised for that purpose in accordance with the Council's Communications and Operation Management





Policy. These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- Determining if communications are relevant to the business.

Where a manager suspects that the email facilities are being abused by a user, they should contact the ICT Manager. Designated staff can investigate and provide evidence and audit trails of access to systems. ICT Services will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee's email is strictly forbidden unless the employee has given their consent, or their email needs to be accessed by their line manager for specific work purposes whilst they are absent. If this is the case then contact the ICT Service Desk. This must be absolutely necessary and has to be carried out with regard to the rights and freedoms of the employee. Managers must only open emails which are relevant.

## **6.6 Categorisation of Messages**

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked in accordance with the HMG Security Policy Framework (SPF). The marking classification will determine how the email, and the information contained within it, should be protected and who should be allowed access to it.

The SPF requires information to be protectively marked into one of 6 classifications. The way the document is handled, published, moved and stored will be dependant on this scheme.

The classifications are:

- Unclassified.
- PROTECT.
- RESTRICTED.
- CONFIDENTIAL.
- SECRET.
- TOP SECRET.

Information up to RESTRICTED sent via GCSx must be marked appropriately using the SPF guidance.



You should refer to Council's Information Protection Policy for full details on the application of information classification.

## 6.7 Security

Emails sent between Scarborough.gov.uk address are held with the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, PROTECT and RESTRICTED material must not be sent via email outside a closed network, unless via the GCSx email.

Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT and RESTRICTED material.

**All Council employees that require access to GCSx email must read, understand and sign the GCSx Acceptable Usage Policy and Personal Commitment Statement.**

## 6.8 Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under GDPR/Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure of whether they should pass on information, they should consult their line manager.

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of Scarborough Borough Council.

Care should be taken when addressing all emails, but particularly where they include PROTECT or RESTRICTED information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent PROTECT or RESTRICTED material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the ICT Service Desk in the first instance.



The automatic forwarding of a GCSx email to a lower classification email address (i.e. a standard .gov.uk email) contradicts national guidelines and is therefore not acceptable.

## **6.9 Negligent Virus Transmission**

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of the Council's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to ICT Service Desk.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access Council facilities.
- Must not forward virus warnings other than to the ICT Service Desk.
- Must report any suspected files to the ICT Service Desk.

In addition, the Council will ensure that email is virus checked at the network boundary and at the host.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Council's Software Policy.

## **7 Policy Compliance**

Any potential misuse or abuse of this policy identified from monitoring or other means will be reported to the Director/Monitoring Officer and the Human Resources Manager and an investigation may then be carried out. Serious breaches of this policy will normally be regarded as gross misconduct. Breaches of this policy may therefore result in disciplinary sanctions up to and including dismissal. Any such breaches may also be criminal offences and may therefore lead to prosecution irrespective of any disciplinary action that might be taken. Breaches of the policy shall be dealt with under the Council's Disciplinary Procedure as appropriate.

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT Services or HR.

## **8 Policy Governance**



The following table identifies who within Scarborough Borough Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<b>Responsible</b>	ICT Manager
<b>Accountable</b>	Chief Executive
<b>Consulted</b>	Human Resources, ICT Operational Group, Consultative Panels
<b>Informed</b>	All Council Employees, Councillors, Temporary Staff, Contractors

## 9 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the ICT Manager.

## 10 References

The following Scarborough Borough Council policy documents are directly relevant to this policy, and are referenced within this document :

- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Software Policy.
- Communications and Operation Management Policy.
- Corporate Data Protection Policy.

The following Scarborough Borough Council policy documents are indirectly relevant to this policy :

- Internet Acceptable Usage Policy.
- ICT Access Policy.
- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Removable Media Policy.



- Information Protection Policy.
- Information Security Standards Policy - Managers Responsibilities.
- Information Security Incident Management Policy.
- ICT Infrastructure Policy.
- Secure Transfer of Information Policy.

## 11 Key Messages

- All emails that are used to conduct or support official Scarborough Borough Council business must be sent using a “@Scarborough.gov.uk” address.
- All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format “@Scarborough.gcsx.gov.uk”.
- Non-work email accounts **must not** be used to conduct or support official Scarborough Borough Council business.
- Councillors and users must ensure that any emails containing sensitive information must be sent from an official council email.
- All official external e-mail must carry the official Council disclaimer (see section 6.1).
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council’s Equal Opportunities policy.
- Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT and RESTRICTED material.
- Automatic forwarding of email must be considered carefully to prevent PROTECT and RESTRICTED material being forwarded inappropriately.



## **Appendix 1**

For procedures on the use and best practice on email usage see the Council's Email Usage Guidelines.

While email is often credited with revolutionising business communication and enhancing productivity, the sheer volume can undermine these benefits. Additionally, as the use of email messages increases, both internally and to third parties via the Internet, Scarborough Borough Council faces a number of risks.

These guidelines must be followed at all times to minimise the business risks and maximise the benefits of email usage within Scarborough Borough Council.