Q2

POLICY AND GUIDELINES ON THE USE OF ELECTRONIC MAIL (EMAIL)

Lead Directorate and Service:	Corporate Resources / Human Resources
Effective Date:	November 2016
Contact Officer/Number:	HR Advice Centre/391221
Approved by:	The Cabinet: 14.3.05 Min: 2185/11.12.07 Min: 3147. CMT 1.3.10 Min No: 12308 DR 10783/ CMT 11.2.13 Min: 14839, DR 14271/ CMT 8.9.14 Min: 15911, DR 16170/ 14.11.16, DR 18730

Policy on the Use of Electronic Mail (Email)

1. Scope

1.1 This policy and guidelines apply to all employees of the Council where E-mail access is via the corporate network, including school based employees where it has been adopted by the respective school governing body. This includes all associated messaging facilities within the E-mail system.

2. Background

2.1 The East Riding of Yorkshire Council has an electronic mail system which allows employees to send and receive messages and allows attachments such as word processing documents and spreadsheets to be sent with the message. Additionally email can be sent to, and received from, all Internet users worldwide.

2.2 Well publicised cases of defamation, sexual and racial harassment and downloading of obscene materials by email/Internet have led to many employers regularly monitoring use of their systems. With the Regulation of Investigatory Powers Act 2000, Human Rights Act 1998 and the Data Protection Act 1998 (Part III), employers have a number of different considerations to take into account. These Acts require them to constantly refresh their existing practices against new technologies for communication and employees rights.

3. Policy Statement

3.1 This policy and guidelines have been produced to ensure that Council employees are fully aware of the rules concerning the uses of the Council's email facility. Email facilities are provided as a **business tool** whether via a desktop/laptop facility or mobile device to enhance communication of work related issues. It is a good cost-effective way of allowing employees to communicate quickly and effectively and should be used primarily for this purpose. All users of email facilities will be accountable for the content of messages sent.

4. Responsibility

4.1 All Directors', senior managers' and delegated managers' will be responsible for ensuring that the policy is applied consistently within their Directorate. As part of the induction process an employee must be made fully aware of the policy. The employee's manager must discuss the policy with the employee to ensure the employee understands its content.

4.2 An employee is responsible for reading the Policy and Guidelines on the Use of Email at the start of their employment and should ensure any concerns or queries are raised with their manager prior to accessing the email system.

5. Policy Review

5.1 This email policy will be reviewed in line with the Council's rolling policy review programme by Human Resources and the Corporate ICT Section in consultation with relevant departments and recognised Trade Unions.

6. Links to Other Policies/References

Disciplinary Policy and Procedure
IT Security Policy
Policy and Guidelines on the Use of the Internet
IT Security Incident Response Procedure
Data Protection Policy
Mobile Device Policy and Procedure
Social Media Guidelines
Data Protection Act 1998
Freedom of Information Act 2000
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Equality Legislation

<u>Guidelines on the Use of Electronic Mail (Email) Services</u>

1. Introduction

1.1 The use of email and the Internet is changing the way that the Council is communicating with itself and with others. The use of these technologies is a means of improving the way that the Council communicates and will be encouraged. However, the following guidance **must** be followed:

2. Acceptable Use of Electronic Mail

2.1 Email is recognised as a proper method of communication within the Council but must not be used as a way of avoiding traditional means of communication.

2.2 Email is the equivalent of a written document and is used as an evidential record of vicarious liability for defamatory statements. Extreme caution must be exercised in the style, content and language used, it must be at all times 'business like'.

2.3 Messages which are abusive, defamatory or make improper or discriminatory reference eg to a person's race, colour, religion or belief, gender, age, nationality, ethnic origin, disability, marital status, pregnancy, sexual orientation, gender reassignment, HIV status, Trade Union involvement or political activities must not be distributed. Users must be sensitive to the views of others, and email must not be used to harass anyone in any manner.

2.4 It is easy to unintentionally write an email in a threatening manner. Employees must take care not to send aggressive emails which are often referred to as "flame" mails. A "flame" mail is generally a response that is sent in the heat of the moment and conveys emotion or feeling which may not be appropriate. It is advisable that employees should allow the situation to "cool down" before responding.

2.5 Employees are prohibited from sending unsolicited, irrelevant or inappropriate email to other employees, to newsgroups or mailing lists on the Internet or making any excessive use of unsolicited mail. Moreover, participation in chain, pyramid letters or similar schemes is prohibited. Any chain mail sent to the Council must NOT be replicated across the network. Anyone receiving this type of email must immediately inform the IT Service desk on (01482) 394444.

2.6 Employees should not:

- sign up to any mailing lists or newsletters unless they are work related
- use their Council email address as a primary address for making purchases of goods and services from the internet
- use their Council email address on eBay, PayPal, Amazon or similar or to pay for personal purchases
- forward emails classified as Official or Sensitive under the Councils Protective Marking Scheme to a personal or non-Council email accounts for the purpose of remote working.

2.7 Employees who receive messages informing them of viruses or other security threats must only forward the information to the IT Service Desk IT.Servicedesk@eastriding.gov.uk Most messages of this nature are hoaxes, designed to disrupt email services by generating unnecessary traffic.

2.8 Employees receiving emails that could be deemed inappropriate or excessive should contact their Line Manager in the first instance and where appropriate inform the originator of the inappropriateness of the email.

2.9 When dealing with email enquiries, employees should not normally offer help in areas which are not within their remit, but should forward the message to a relevant person. It is good customer care to inform the originator of the email that you have forwarded their request to a colleague and provide the name and contact details of the employee. Employees must not give advice or information known to be contrary to the Council's policies or interests.

2.10 Email is one of a number of methods for the transmitting of viruses and malicious programs and copyright material. Employees must ensure that no contravention of third-party copyright takes place. For employees with Council supplied computers, connected to the Corporate Network, any anti-virus software will be automatically updated by IT. Any employee uncertain about this should contact the IT Service Desk.

2.11 The Council has systems in place to prevent users from receiving spam emails, but if any spam is received users are encouraged to forward the email to the spam reporting email address; Spam Reporting which is listed in the East Riding address book. To minimise the risk from computer viruses, the following practices are recommended to prevent virus problems:

- Always run the corporate standard, supported anti-virus software.
- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, and empty your Trash.
- Delete spam, chain, and other junk email without forwarding, in accordance with the Councils Policy and Guidelines on the use of Electronic Mail.
- Never download files from unknown or suspicious sources.
- Always scan portable media from an unknown source for viruses before using it.
- New viruses are discovered almost every day. Ensure your antivirus software is up to date.

2.12 Excessively large emails or attachments (greater than 10Mbytes) should be avoided to reduce forwarding delays for other email users. Care should be taken when sending mails greater than 3Mbytes and assurance should be sought to ensure the large mail can be handled by all the recipients prior to sending. The sending of bulk emails to a large number of external recipients should be kept to a minimum and where possible sent at the end of the working day. If you experience specific difficulties with this facility please contact the IT Service Desk for assistance.

2.13 Target emails only to those people who need to see them, avoid addressing or copying emails to multiple addressees unless absolutely necessary. If you do need to send messages to multiple addressees make it clear whether action is required from all or some of the addressees or if it is for information purposes only.

2.14 Care should be taken when sending emails to multiple recipients. To send an email to a recipient without revealing their address to the others, the addresses should be added in blind carbon copy (bcc) field, not carbon copy (cc). When using cc every recipient of the message will be able to see all the addresses it was sent to. It is particularly important to use bcc when sending emails to multiple recipients who are not involved in their professional capacity eg when sending a newsletter or questionnaire to service users.

2.15 The email system should not be used as a file storage system. Attachments should be saved to home or group folders on the corporate file storage wherever possible and the email should then be deleted.

2.16 The corporate standard for email account mailbox size is 300Mbytes and the email system automatically issues a warning when the mailbox reaches 250Mbytes. Employees should delete old unwanted emails to ensure that this capacity is not breached.

2.17 Every email account has an archive facility, which is managed by the account owners. Employees should ensure that this facility is managed and that only those emails that are essential to keep are kept.

2.18 Emails are archived automatically after 30 days and when they are archived the attachments are removed. Users should store all attachments on file servers (see 2.17).

2.19 The global email facility available on the Council's email system is an important communication tool. It is used to get important information, primarily in relation to accommodation, or IT information across to employees and Members. However, issuing global emails does have an impact on the performance of the system and as a consequence global email use is normally restricted to corporate policy, property and ICT matters that need to be communicated across the Council. Other matters which fall outside these definitions should be referred to the Director of Corporate Strategy and Commissioning for approval.

2.20 All requests for global email should be made to the IT Service Desk via email who will seek approval from the Section Heads within Resource Strategy. Employees should not issue global emails via any other route.

2.21 All users of email facilities will be held accountable for the messages sent from their account, and must ensure that password controls prevent usage by another party. If a user has any suspicion that someone else knows their email password, they should change it immediately. Users can grant permission to allow colleagues various levels of access to their email; there is no need to divulge passwords to achieve this. The IT Service Desk can be contacted for assistance with this.

2.22 Computer screens and mobile devices must always be locked when a user leaves the immediate vicinity to prevent unauthorised usage of the logged-in email account.

2.23 No reliance should be placed on the delivery of email. Faults in remote areas of the Internet, virus attacks and mail forwarding policies may delay email forwarding for hours, days or even weeks. Users should check that urgent emails have reached their intended recipients by using the trace or error message facility on emails, this can be found in delivery options, alternatively users could telephone the recipient to ensure receipt.

2.24 Under the Freedom of Information Act 2000 a request for access to information held by the Council can be submitted. This will include email and therefore the content of emails must be carefully considered before sending. Section 3 of this document provides further guidance on Email Etiquette.

2.25 The Council is able to recover emails even if the mail is deleted the same day, using the journal facility. If emails are retained or have not been accessed before the nightly backup of the email system is carried out a copy of the email will be retained in the Council's backup system for a maximum of 6 weeks.

2.26 The Council operates an internal instant messaging service (IBM Sametime), this allows users to send short messages instantly to individuals of groups rather than via email. This service should be used following the same guidelines and acceptable use as for traditional email, all conversations are logged and can be monitored.

3. Personal Use of Electronic Mail

3.1 Email facilities are provided as a business tool to authorised Council employees whether via a desktop/laptop facility or mobile device and therefore must not be routinely used for personal purposes. Employees are discouraged from using email for informal private use.

3.2 Any private use must be undertaken in the employee's own non working time ie. before or after their working start and finish time or in their lunch break . An employee's work pattern as entered onto i-Trent will be the definitive record for defining an employee's work/non work pattern. Personal usage of email during an employee's lunch break is limited to a maximum of 30 minutes.

3.3 All personal use must be kept to a reasonable level and may be monitored to ensure compliance. Any excessive or inappropriate personal use could result in disciplinary action.

4. Email Etiquette

4.1 When writing emails there are several Do's and Don'ts that should be followed, which are detailed in the table below:

DO	DON'T
• Consider the message you want to convey. • Always use plain English. • Make sure that the language and style of writing used is appropriate for the recipient. • Type directly into the message box where appropriate. • Ensure that the mailing list is relevant and current and double check before sending. • Use a strong subject line to allow easy understanding of the subject matter. • Proof read emails prior to sending; if you are uncertain about the content get it read by someone else. • Use spell check before sending emails. • Ensure compliance with Corporate Customer Standards. • Use 'Out of Office' messages if you are away for your PC for more than one working day. • Use automatic signatures (see below). • Delete unwanted messages immediately. • Keep messages remaining in your mailbox to a minimum. • Use blind copies sparingly. • Consider the environment before printing emails.	• Use email to break bad news or to discuss tense or confusing information. • Use "text speak" or acronyms. • Use attachments when the detail in the attachment could be typed directly into the message box itself. • Send emails to people who do not require it. • Write the whole message in capital letters, as it is generally termed as SHOUTING. • Do not include humorous remarks, jokes and sarcasm, as the recipient may not interpret them as you intended. • Use return receipts unless it is absolutely necessary. It can be considered annoying and an invasion of privacy. • Use emoticons (keyboard character combinations that convey emotion when viewed sideways eg:-) • Respond to 'All' and 'With History' unless necessary and remember to delete unwanted attachments. • Give anyone your User ID or password; grant the person access to your emails so they can view them from their PC instead. If you require assistance with this contact the IT Service Desk.

4.2 The use of mobile email devices such as Blackberrys, Smartphones and tablets across the Council is increasing as technology develops. Extreme caution must be exercised in the style, content and language used, it must be at all times 'business like'.

4.3 One attribute of email that distinguishes it most from other forms of communication is its ability to sometimes evoke emotion in the recipient.

4.4 Misinterpretation of the content or form of the email message can provoke conflict which was never intended. The ease in which the recipient can then fire off a hasty response often inflames the situation. This expression of extreme emotion or opinion in an email message is known as flaming.

4.5 Unlike telephone and personal conversations that fade with time, impulsive email responses can sit around in mailboxes, be printed out, circulated and acquire a level of importance that was never intended. This is a real barrier to effective communication and can have a negative impact on relationships at work.

4.6 When you receive an email that generates emotion ensure that you:

- Read it again; reassess the message. Resist the temptation to fire off a response.
- If you must, draft a response and let it cool off for a time before sending it. Save it as a draft and then reconsider the response later.
- Read and interpret the original message again.
- Assume the good intentions and competence of the sender.
- Separate opinion from non-opinion while reading a message, you can then respond appropriately.

4.7 A signature file can provide useful information such as a mailing and email information address, phone/fax number, website address or other contact information. Four or five lines are about the maximum. The signature file usually appears at the end of your email message. Think of the signature file as your electronic business card. Signatures can be created via the tools/preferences/signature tab from within the email system.

4.8 Email messages are permanent. Don't be fooled by the informality and speed of email. Even though you may delete the message from your computer to free up storage space, the message can be retrieved from the system. The same rules around harassment and offensive material still apply. Emails will be used in evidence in a court of law and they are covered by the Data Protection Act.

4.9 Remember the Security Policy guidance about Passwords. A password is confidential authentication information composed of a string of characters used to access computer systems. Passwords must be kept confidential. Passwords are the responsibility of individual users. The giving of an authorised password to someone unauthorised in order to gain access to an information system may be a disciplinary offence. No staff should be given access to a live system unless properly trained and made aware of their security responsibilities.

5. **Staff Notice Board**

5.1 The staff notice board may be used for general information, sharing work related social activities or items wanted/for sale.

5.2 Placing and access to messages must be undertaken in the employee's own non working time. See paragraph 3 above.

5.3 The Council does not accept any liability for any goods bought and sold using the staff notice board; purchases are at the sole risk of the purchaser. If there is any doubt regarding the condition of any goods sold through the notice board, it is a matter for the purchaser to seek their own advice. Sellers are reminded that they must give an accurate description of the goods they propose to sell.

5.4 The Council in no way condones any illegal activity such as the sale of counterfeit goods and will co-operate fully with any enforcement agency which expresses concern at any entry on the system. Any item which is deemed to be inappropriate may be removed from the notice board. Staff will be held responsible for any item they add and should therefore consider whether an item is suitable for sale on the staff notice board prior to its inclusion.

6. **Privacy of Electronic Mail**

6.1 There is no guarantee that communications, either internally or on the Internet, are private or that they will arrive at their destination at a particular time, or at all. Users should be aware that confidential, personal or other sensitive information transmitted via email must only be transmitted in a secure way marked up with the appropriate security level. Usually this will be using the governments secure gateway, known as Government Connect or GCSX and transmitted over the PSN network.

6.2 Users are reminded that all email messages are monitored and that random checks will be made. As the use of electronic mail is in respect of the work of the Council, then all users need to be aware that there will be circumstances where it will be necessary to examine the contents of messages and the usage made of the electronic facilities.

6.3 Where there is reasonable belief that the Council's email facilities have been misused specific checks may be made to individual email accounts.

7. Privacy of Electronic Calendars

7.1 Users of the electronic calendar system should be aware that confidential, personal or other sensitive information entered into electronic calendars must only be recorded in a secure way with the appropriate anonymity applied. An example of this could be to use a client's unique reference number (where applicable), or the title of the meeting rather than names, addresses or dates of birth.

7.2 Users of the electronic calendar system should ensure they do not have an open calendar (unless necessary) and only assign access to colleagues who require access for work purposes. This should be reviewed on a regular basis.

8. **Automatic Forwarding of Email**

8.1 Automatically forwarding email should not be used from a Council email account to an outside email account. Automatic email forwarding has the potential to inadvertently transfer sensitive information by employees, vendors and agents operating on behalf of Eastriding. If there is a critical business case for this function, then this request must be via the employee's line manager and be approved by a Head of Service.

9. Incident Management and Monitoring

9.1 IT Services has defined a security incident response procedure. All users must contact the IT Service Desk if they are aware of, or suspect, a breach of the Email Policy.

9.2 The Council will monitor the use of the Email system by staff and reserves the right to inspect all files stored on network servers; PCs and laptops to ensure compliance with the Policy.

10. Misuse

10.1 Any identified misuse of the electronic mail facilities will be investigated and could result in action under the Council's Disciplinary policy and procedure.

10.2 Examples of misuse could include excessive personal or inappropriate use of the system, personal use during normal working hours, inappropriate use of the staff notice board facility, participation in chain/pyramid letters or similar schemes and initiating or forwarding messages which are abusive, defamatory or make improper or discriminatory remarks. The above list is not exhaustive.