Comhairle Ceantair
Lár Uladh
Mid Ulster
District Council

Email and Instant Messaging Policy

Document Control			
Policy Owner	Head of IT, Barry O'Hagan		
Policy Author	Head of IT, Barry O'Hagan		
Version	2.0		
Consultation	Senior Management Team Yes Trade Unions Yes		
Equality Screened by	Yes	**Date**	June 2020
Equality Impact Assessment	Yes	**Date**	June 2020
Good Relations	N/A	**Date**	N/A
Approved By	(Policy & Resources)	**Date**	TBC July 2020
Adopted By	Council	**Date**	TBC July 2020
Review Date	July 2022	**By Whom**	Head of IT
Circulation	Councillors, Staff, Intranet		
Document & legislation Linkages and	Internet Use policy Mobile Phone Policy The Privacy and Electronic Communications Regs (PECR) Dignity at Work Policy Social Media Policy Regulation of Investigatory Powers Act 2000 Lawful Business Practice Regulations Code of Conduct for Councillors Data Protection Policy & Legislation Information retention & disposal Policy Code of Conduct for Council Employees Communication Strategy Communication Policy Freedom of Information Policy &Legislation Language Policy Disciplinary Policy		

Contents

1.0 Introduction

Email and Instant messaging are critical communications and collaboration services for Mid Ulster District Council (MUDC) for transferring and sharing information if both sender and recipient are aware of the classification of the information and the safest way to send it. These systems are managed by Information Technology (IT).

2.0 Policy Aims & Objectives

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

- Providing guidance on how to use instant messaging and email in a safe and appropriate manner that protects personal data and the organisation information systems.
- Informing users about the acceptable use of the systems.
- Stating the actions that may be taken to monitor the effectiveness of this policy.

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

3.0 Policy Scope

This policy covers all email, collaboration and messaging systems and facilities that are provided by Mid Ulster District Council for the purpose of conducting and supporting official business activity through the Councils network infrastructure, mobiles and all stand alone and portable computer devices.

This policy is intended for all Mid Ulster District Councillors, Employees of the Council, contractual third parties and agents of the Council who have been designated as authorised users of messaging facilities.
System examples include Microsoft Office, Outlook, Skype for business, Teams, Cisco Jabber, Cisco WebEx, Skype, Portal administration tools.

4.0 Linkage to Corporate Plan (2020-2024)

The policy is aligned with the corporate themes

Theme 1: Leadership
This theme is intended to reflect the Council's position as an organisation which has a key role to play not only in the direct delivery of services which will impact positively on people's lives, but also as a key shaper and influencer externally.

Theme 2: Service Delivery
In this theme, we focus on our internal agenda in terms of our resources (people and finances) and the priorities which will ensure we are a high-performing Council, where excellence is standard.

5.0 Roles and Responsibilities

All Staff have a responsibility to adhere to the guidelines contained within this policy and abide by the Code of Practice for Email and Instant messaging (“ Acceptable Use”) in appendix 2.

Managers at all levels are responsible for ensuring that their relevent staff have read and understand their obligations in relation to this policy.

It is the responsibility of each individual user to ensure that they use Council’s IT services in an acceptable manner in accordance with all policies and current legislation.

The ICT service will be responsible for the implementation of technical controls and review of this policy including .

- Managing/reviewing/analysing fault calls/issues
- Administering access to Council information systems
- Managing/reviewing/analysing security breaches

6.0 Procedure and Implementation

General Policy statement

Purpose: Email and Instant Messaging as a form of Communication

Email and instant messaging 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 or instant messaging intended. It is therefore the responsibility of the person sending an email to decide whether it is the most appropriate method for conveying information.

Instant Messaging and Collaboration tools are a handy tool for quickly checking information or arranging a short notice meeting and team work but should not be used for communicating financial information, authorisations, decisions, historic or other information that must be retained for statutory or Council purposes e.g. it may be needed in a response to an FOI request or be part of an audit trail.

Instant messaging should only be used for informal communications with colleagues - any discussions pertinent to the Council’s business should be conducted via email so that a formal record exists.

IT facilities provided by the Council for email and instant messaging should not be used:

- for any unlawful endeavours including hacking.
- to request or provide any copyrighted material in a way which would infringe the rights of the copyright holder.
- for advocacy of any religious or political cause.
- In any way that breaches council policies and procedures relating to dignity at work or that could cause offence on any grounds covered by equality and anti-discrimination law (age, religious belief, political

opinion, gender/gender reassignment, pregnancy/maternity, disability, race, sexual orientation, marital status or dependency).

- Access inappropraite or offensive material e.g Pornographic material etc.
- Remarks which are derogatory or defamatory towards any person
- The sending of bulk email/IM, including excessive use of mailing lists, which is unrelated to the legitimate activities of the Council and is likely to cause offence or inconvenience to those receiving it.
- The sending of sensitive messages using email/IM, for example employment decisions. If in doubt, alternative methods of communication should be employed, or advice sought.
- Subscribing to external web sites and mailing lists using your Council email address for personal use not related to your Council work. For example: Amazon, EBay, etc.

Whilst it can sometimes be helpful to maintain a chain of e-mails on a particular subject, long chains of e-mails are best avoided. Information from e-mails may be required to answer Data Protection/FOI requests and difficulties can arise if a chain of e-mails refers to data which should not be disclosed. Users should consider this when responding to or creating an e-mail chain and, where appropriate, create a fresh message.

The Council's Social Media Policy provides further guidance relating to unacceptable use of email & Internet with respect to the use of Social Networking (for more information please see the Social Media Policy on the intranet).

Security and Risk

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

These include;

Loss of Council Information
Financial penalties for failing to meet legal obligations
Risk to the safety and privacy of service users
Impact on the ability to share information with other bodies
Damage to the Council's reputation
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.

All emails arriving at the Council are subject to technical controls and scans for computer virus and (unsolicited bulk email/spam) content before delivery, manual intervention or rejection. These control systems can never be 100% accurate.

Some guidelines are listed below to minimise risk but the full code of practice is detailed in appendix 2. Contact the ICT Service Desk if you require advice:

i Do not open attachments received from unsolicited or untrusted sources;

ii Be wary of unsolicited attachments. If in doubt, contact the sender or IT services to check before opening the attachment;

iii Do not email/IM attachments known to be infected with a virus;

iv Check that suitable anti-virus software is installed on the computer you're using and that it's up-to-date;

Although the Council uses (where available) secure methods for email transmission and user access, email confidentiality cannot be guaranteed. Unless special measures are undertaken by the user, all emails should be regarded as insecure. Personal, confidential or sensitive information should not be sent in the body of an email. Where there is a business need to send personal, confidential or sensitive information via email then the information must be encrypted before it is attached to the email.

For guidance on how to encrypt and protect documents please contact the ICT Service Desk or consult the intranet learning section.

Credit card information

Credit Card Information must never be sent via email/IM or asked to be sent via email/IM. Any credit card information received via email/IM must be immediately deleted by the recipient and must not be printed, copied, replied to, forwarded on or processed for payment. The sender must be informed that no payment was taken, their credit card details were deleted and that they must use an approved method of payment. The incident must also be reported to the IT Service Desk as there are further processes needed to remove the data from our systems.

Email as Records

Emails and Messages are a form of record keeping as well as a means to communicate. Accordingly, they should be treated and managed as an informational asset.
Information held on Council equipment is considered to be part of the corporate record and provides a record of staff activities.

Non-work email accounts **must not** be used to conduct or support official MUDC business. Councillors and users must ensure that any messages containing sensitive information are sent from an official council email.

Ownership & Monitoring

The associated user accounts and their stored data within the Councils Email and IM systems are the property of the Council which allows the Council the right, where necessary, to monitor/access emails and IMs.

Data Protection and Freedom of Information

As well as the guidelines outlined in the ICT Security Policy and the Data Protection Policy, the following guidelines are specific to email and logged IM chats:

1. The use of email, as a means of internal as well as external communication, falls within the provisions of the Data Protection Act 2018;

2. Under the Data Protection Act, all email transmissions and logged IM chats which contain personal data may be disclosed in response to a request for

disclosure, brought forward (through normal procedure), via the Councils Data Protection Officer.

3. The Councils internal and external use of email systems, for bona fide purposes connecting with its operations, is registered with the Data Protection Registrar;

4. Under the terms of the Data Protection Act 2018, email users who have access to email addresses have a responsibility not to disclose email addresses or email distribution lists (Personal Data) to an unauthorised third party without permission of the owner of the email address.

Emails and logged IM chats are also potentially subject to disclosure under the Freedom of Information Act.

Classification:A Requirement to maintain Integrity and confidentiality

Asset classification and control is an essential requirement, which will ensure the Confidentiality, Integrity and Availability of information used by the Council. An information classification system is used to define appropriate protection levels and to communicate the need for special handling measures. Each information asset is classified to indicate its sensitivity and to identify the controls required to protect it.

The Council's Classification Scheme

The Council will only be using the OFFICIAL classification. However, the OFFICIAL classification also includes a handling caveat of OFFICIAL-SENSITIVE in order to identify information that should only be available on a strictly need to know basis and may need additional measures of protection. These classifications should be applied to all information including emails, paper documents, electronic documents, systems etc.

All Council information will be classified as OFFICIAL unless there are specific handling requirements.

Any information that is not marked will be assumed to be OFFICIAL
All staff are under a general requirement to maintain the confidentiality of information.

There are also particular responsibilities under 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 or the Head of IT for further advice.

Care should be taken when addressing all emails, but particularly where they include SENSITIVE or RESTRICTED information, to prevent accidental transmission to unintended recipients.

Sensitive Information and Email

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. The classification will determine how the email, and the information contained within it, should be protected and who should be allowed access to it.

There are several ways to mark emails – it is down to the discretion of staff to decide which the best way for them to do this is. It is possible to use Outlook to mark emails as 'Private' or 'Confidential' – guidance on how to do this can be found on the intranet. Alternatively, staff can include the classification of the information in the subject line of the email, this would be seen before the recipient sees the body of the email. It is imperative the recipient of any SENSITIVE or RESTRICTED information is aware that this is the classification of the information.

Instant messaging should never be used to communicate PROTECTED or RESTRICTED information.

The OFFICIAL-SENSITIVE caveat should be used at the discretion of staff depending on the subject area, context and any statutory or regulatory requirements where it is particularly important to enforce the need to know rules.

However, the caveat should be used by exception in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know' as compromise or loss could have severe and damaging consequences for an individual (or group of individuals), another organisation or the Council more generally. This might include, but is not limited to the following types of information:

- The most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- policy development and advice to members on contentious and very sensitive issues;
- commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to the Council or to a commercial partner if improperly accessed;
- Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- more sensitive information about security assets or equipment that could damage capabilities or effectiveness;
- very sensitive personal data that would be extremely damaging to an individual if lost or compromised, e.g. child protection cases, HR compromise agreements,
- Government data where they have defined it as OFFICIAL-SENSITIVE and insist on strict sharing protocols

OFFICIAL-SENSITIVE data cannot be shared externally except through an approved secure email system/secure network or appropriate data encryption and password protection and should be accompanied by a defined distribution list. Data sharing with external organisations must be in line with corporate data sharing agreements or contract terms.

Where large volumes of OFFICIAL-SENSITIVE information about particular topics are regularly shared between organisations, the respective information asset owners will need to agree specific handling arrangements and transfer protocols in line with the policy.

Retention

The council will retain a copy of emails within an email archive in line with the Council's information retention and disposal policy/schedule. Individual access to the archive is provided through the intranet (my apps).

Mail on Mobile devices

MUDC Mail allows for the synchronisation of emails, calendar, tasks, contacts and other mailbox features to a mobile device such as a smart phone.

It must be recognised that these devices are more susceptible to theft and/or loss and therefore staff must adhere to the following:

Only approved mobile phones devices must be used to synchronise MUDC Mail Accounts to. Approved devices have been selected to ensure that safeguards are in place to protect any data downloaded to the device e.g. the use encryption and PIN numbers.

Staff wishing to synchronise their MUDC Mail accounts to their personal mobile phone must comply with the criteria set out in this policy and acceptable use policy.

Staff must only request the functionality required to undertake their job role e.g. if only calendar access is required then staff should not request all mailbox functionality to be synchronised to the device.
Due to their relatively small size staff must take extra care when responding to emails or sending an email message from a mobile device, especially with regard to ensuring that the correct email recipient has been selected. These devices usually have very small key pads or on screen keyboards which make it easy to input an incorrect character which may result in the misdirection of an email.

Any loss of a mobile device being used to synchronise a MUDC Mail account must be reported to the ICT Service Desk at the earliest opportunity so as to minimise the risk of loss of data.

Monitoring of Email and IM Usage

All users should be aware that messaging and email usage is monitored and recorded centrally. The monitoring of (outgoing and incoming) traffic will be undertaken so that 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.
- Complies with informational security and legislation requirements.

Whilst respecting the privacy of authorised users, under the Data Protection Code of Practice, Council maintains its legal right to monitor and audit the use of email by authorised users under the Lawful Business Practice Regulations 2000. 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.

Note: IM conversations are not routinely retained or archived, but may be forensically recovered if required for criminal or disciplinary investigation purposes in accordance with the above authorisations.

Access to another employee's email is **strictly forbidden** unless: - (a) the employee has given their consent, (b) their email needs to be accessed by their line manager for specific work purposes whilst they are absent or (c) an appropriately authorised investigation is being undertaken.

In the case of (b) and (c) authorisations must be obtained from the corresponding Director or Chief Executive.

Access granted to email and network accounts must be for a specific purpose and **proportionate to the need** having regard to the rights and freedoms of the employee and the expectations of a reasonable level of privacy with regard to personal communications. Managers must only open emails which are relevant to the business need and/or purpose stated.

Shared Mailboxes

Where several users are responsible for the same area of work and require access to the same emails then a member of the Head of service may ask/request for a shared mailbox with an associated, generic, email address that represents the shared area of work to the ICT Service Desk. The request must include the names of at least 2 staff who will be in overall management of the shared mailbox and any other names of users who require access before it is considered and approved.

An email address allocated to a shared mailbox must be generic enough so that it encompasses the area of work shared by the users accessing that mailbox but it must not be so generic that there would be an overlap with users performing a similar role in another part of the Council who would not have access to that shared mailbox.

A shared mailbox does not have an associated username and password as users must log on with their personally-allocated username and password. This will give them access to their own mailbox and to the shared mailbox.

Out-of-Office Message, Disclaimer and Signatures

Staff users must set the Out-of-Office option when they are away stating an alternative email contact for work-related matters.

Each email leaving the organisation should include a compliant signature as prescribed in Appendix 3.

Emails sent by staff to recipients outside the Council will automatically include an approved disclaimer (as per appendix 1)':

Account Activation and Termination

Account changes for staff to receive email services must be made in writing through the ICT Help Desk by a head of service or human resources.

Staff mailboxes and messaging accounts will be deleted at the termination of the staff member's employment.

Where explicitly requested in writing by a head of service, a mailbox of a staff member who has left may be kept open for a period of not more than two months, with an Out of Office reply directing enquiries to a different email address.

Any email addressed to a named staff member who has left may NOT be redirected to another email address. Such emails may contain personal, confidential or inappropriate content that may place the Council or Staff at risk if it is opened.

Staff mobile devices which are used to connect to MUDC provided mailboxes or which contain data owned by or held by the Council will be wiped at the termination of a staff member's employment.

Web based Email

Mid Ulster District council's email can be accessed from any computer or device with internet capabilities and the required security measures. The web based version of MUDC email can be accessed by navigating to https://login.microsoftonline.com/

Policy Compliance

If any user is found to have breached this policy, they may be subject to Mid Ulster District Council's disciplinary procedure.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT services.

In the event of an accidental breach of this policy staff members must advise their line manager immediately so that appropriate steps can be taken to mitigate or remove any possible risk(s) e.g. the exposure and/ or loss of sensitive data.

7.0 Impact Assessment & Screening.

The policy has been rescreened using Mid Ulster District Council's Equality Scheme and Rural needs Assessment templates.

Staff and financial resources
The systems to implement and provide email, messaging and monitoring are provided and resourced through the IT services budget and resources.

The primary systems are Office 365 and Teams & Cisco Jabber requiring internet access and network connectivity to back office telephony.

8.0 Support and Advice

For further information and advice about the policy, please ICT ,
Service Desk Internal extension 22222
Or alternatively Head of IT: Barry O'Hagan: Ext 23312.

User Training and Support

New start will receive training as part of on-going inductions for new staff affected.

Implementation of the policy may require the release of staff across the organisation to be briefed via team meeting and updates.

Users will be provided with the following support, guidance and training materials on the intranet:

Policy
Policy Summary
Code of Practice for Email & Instant Messaging
O365 Microsoft learning Paths Online

9.0 Communication

The policy will be communicated internally using a range of appropriate internal communication methods, team meetings and on the council intranet.
The policy will also from part of the induction process for all new staff.

10.0 Monitoring and Review Arrangements

The effectiveness of the policy will be monitored using feedback from those staff involved in its implementation and data collated on performance against standards.

Formal review, with any appropriate recommendations for change, will take place 2 year after implementation unless changes in legislation prompt an earlier review.

Appendix 1

Email Disclaimer on all email leaving the organisation;

'This email is solely intended for the recipient identified above ('intended recipient'). The contents of this email are confidential and may be subject to legal professional privilege. Only the intended recipient may rely on the contents of this email. The contents of this email do not express the views of Mid Ulster District Council ("the Council") unless otherwise clearly stated. The sender (including the Council) cannot guarantee that this message or any attachment is virus free. Any person who opens or otherwise accesses an email from the sender in the future does so at their own risk and acknowledges and agrees that the sender (and the Council) is not responsible for any loss or damage suffered by any person.

Privacy Information

As a public body, the Council may be required to disclose this email (or any response to it) under Data Protection and/or Freedom of Information legislation, unless the information contained is covered by an exemption. The Council treats your personal data in compliance with the legislation. To learn more about how your data is processed please go to www.midulstercouncil.org/privacy. If you receive this email in error, please immediately report the error to the sender and permanently delete this email from all storage devices.'.

Appendix 2

Code of Practice for Email and Instant messaging ("Acceptable Use")

All users should adhere to the following guidelines for appropriate use:

Check your email regularly - once a day is an absolute minimum. For staff users, depending on the nature of the post, email may need checking on a more regular basis. Staff must recognise that certain communications may be time critical.

Do not expect a recipient to be constantly checking their email/IM or be available to respond immediately. If you require an immediate response, then email/IM is not the correct method of communication and you should use a phone call instead.

If you use the 'Urgent' feature in email then it lets the recipient know that you consider the matter to be urgent. However, the recipient has their own workload to manage and, as such, the email may not be deemed urgent by them.

The use of 'Delivery Receipt' or 'Read Receipt' on an email can be deemed to imply a lack of trust in the recipient and so should not be used unless absolutely necessary. It should be noted that a 'Delivery Receipt' or 'Read Receipt' response is not guaranteed and may be blocked by the recipient's email system or the recipient's email client.

Be polite. Messages sent by email/IM can often seem abrupt, even when this is not the intention. Use professional courtesy and discretion. The use of all upper-case text in either the subject or the body of an email/IM should also be avoided as this is deemed to be the equivalent of shouting;

Before you send an email/IM, read it through to make sure it really does say what you want it to say;

Do not say anything in an email/IM that you would not be prepared to say to someone face to face;

The 'Subject' line must be clear and concise.
The body of the email should be as brief as possible and clear and unambiguous.

All emails that are used to conduct or support official Mid Ulster council business must be sent using a "@midulstercouncil.org" address.

Do not reply "With History" if it is not necessary especially if it incorporates a large attachment. Use 'reply all' and distribution lists with caution in order to keep the number of messages to a minimum and reduce the risk of sending messages to the wrong people;

Messages should be addressed to those from whom an action or response is expected, 'Cc' or 'Bcc' should be used for other recipients for whom the message is for information only;

Respect peoples' privacy and consider this aspect before forwarding messages;

Do not try to carry out confidential or sensitive tasks or express controversial views via email/IM;

Enter a meaningful title in the 'Subject' field at the top of an email to help the reader anticipate the content correctly. Try to keep to one subject per message to help avoiding unnecessary confusion;

Don't use all or part of someone else's message without acknowledgement.

Don’t edit someone else’s message without making it clear what the changes are that you have made. Don’t distribute other people’s messages without permission;

Avoid subscribing to unnecessary mailing lists. Unsubscribe from mailing lists when they are no longer required;

Do not forward email/IM “chain letters”. These are emails/IMs which either ask you to forward them on to all your friends (or to everyone you know) or which state that something bad will happen if you do not forward them. Emails/IMs of this type, which are warning about something (e.g. computer viruses), are almost certainly hoaxes. If you are unsure about any email/IM that you’ve received then contact the ICT Service Desk for information and help.

Staff are required to use the approved Council email signature for all email communications as set out in appendix 3.

No other information should be added to email signatures.

Staff users should ensure that their calendar in the Councils email system is kept up-to-date so that colleagues can easily confirm their availability when booking appointments and arranging meetings.

Mail Box Housekeeping

Delete unwanted or unnecessary email. It is the user’s responsibility to manage their email folders and keep within the set quota limits.

It is good practice to manage email accounts like any other filing system. - On receiving an email users should try to either respond and delete, save or delete it.

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 addresses is discouraged and should only be sent following direction from the Head of Communications and Marketing.

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 and network access permissions allow, then a reference to where the file exists should be sent rather than a copy of the file.

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.

Be wary of how you use your midulstercouncil.org email address – it should only be used for recognised professional bodies and official communications.

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 council facilities or messaging systems.

If the event with issues of repetitive Junk email or spam please contact the ICT service desk for assistance.
The use of COUNCIL-provided email is subject to all relevant laws, policies, and codes
Of practice and guidelines. All users must comply with the COUNCIL’s *Information*

Security Policy, the *Data Security Policy* and the '*code of practice here.*

Personal use
COUNCIL email services are provided to staff, and approved third parties to conduct official Council-related business. Personal emails may be sent using the COUNCIL system so long as they do not breach any policy, Code of Practice and or other terms and conditions of employment.

Employees must regard this facility as a privilege that should normally be exercised in their own time without detriment to the job and not abused. Inappropriate or excessive personal use may result in disciplinary action and/or removal of email facilities. Staff should be aware that email will be subject to monitoring. There is no absolute right for staff to use the email facilities for personal use.

Staff are **not** permitted to access non-council email on Council Systems as they present a security risk.

Council Business

Official COUNCIL business should not normally be conducted from email accounts other than those provided by the COUNCIL. Although it is recognised that this might be necessary in some exceptional circumstances, users should be also be aware that the use of third-party email providers for COUNCIL work may breach contractual, legislative, ethical and policy requirements.

Simple "DO NOTS"

Users must not send messages or message content that may harass or offend , e.g., harass or offend on any ground covered by equality and anti-discrimination law (religious belief, political opinion, gender/gender reassignment, pregnancy/maternity, race, disability, age, sexual orientation, marital status or dependency) or which may be defamatory or obscene.

Users must not send messages from someone else's account except under proper "delegate" and "send on behalf of" arrangements which retain individual accountability.

Users should not normally "auto forward" mail to a non-COUNCIL email system (this includes internet email systems such as Hotmail or Gmail)

Users should not normally enter into contractual agreements by email.
Users must not use COUNCIL email for personal gain or profit.
Users must not use COUNCIL email to represent themselves as someone else.
Users are encouraged not to use COUNCIL email as a means of storing information. All important information should be stored within the network drive
Attachments should be detached from messages and saved appropriately.
Users must not attempt to access personal email accounts (e.g. Gmail or Hotmail) on the Councils network.

COUNCIL email should not be accessed by any end user device that has been deliberately or knowingly cracked or jailbroken, or that may otherwise prove a threat to the Confidentiality, Integrity and Accessibility of COUNCIL user accounts, networks and data.

Under the terms of this policy no person shall monitor another user's email account unless written authorisation has been granted to do so. The monitoring and or inspection of email accounts may only occur in accordance the *Information Security Policy* and the *Monitoring and Logging Policy*.

The COUNCIL, in accordance with its legal and audit obligations, and for legitimate operational purposes, reserves the right to access and disclose the contents users' email messages.

Email Distribution Lists and Mass Emails

Email distribution (group) lists provided by the Council must only be used for matters of Council business. To send to such a distribution list the sender must be either an administrator/moderator of the distribution list. Any multiple use of email distribution lists provided should be avoided unless absolutely necessary;

A valid 'Reply-To' address must be used on any mass email with additional contact details given in the body of the email.

Do not put the name of the distribution list or a large list of names in the 'To' or 'Cc' fields but use the 'Bcc' field instead. This ensures the list of recipients will not be displayed when the email is sent out and prevents recipients from accidentally sending their reply to the whole list.

Do not send mass emails with attachments but try to contain the information within the body of the email or, as a last resort, in a web link. Where a web link is used then it must also provide information as to how the linked content can be accessed manually without clicking on the link. This is to help the recipient distinguish the email from a malicious 'phishing' email.

The email distribution lists are maintained by ICT. Any request for change must be made through the helpdesk.

Web based Email

Mid Ulster District council's email can be accessed from any computer or device with internet capabilities and the required security measures. The web based version of MUDC email can be accessed by navigating to https://login.microsoftonline.com/

Appendix 3

MUDC Email Signature

Email signatures should contain the following information.

Name
Job Title
Telephone Number
Mobile Telephone Number
Provide | Location Address |
Email Address

The font must be Arial 12.

Directorate/department specific additions/amendments to this format must be approved by the Head of Communications and marketing.
The Council Logo with Full text is optional as this requires email to go out as HTML format and should be no wider than pixels and maintain in the correct aspect ratio as per the Council Branding Guidelines available on the intranet.

Maximum Actual Size