**Manchester City Council**
**Report for Resolution**

**Report to:** Personnel Committee – 13 September 2017

**Subject:** Internet and Email policy

**Report of:** Director of HROD

---

## Summary

This report presents an updated Internet and Email policy which has been revised following the launch of Google's G Suite across the organisation. The policy acts upon feedback received as part of the roll out of G Suite across the organisation and updates the current iteration in light of the new technology. Key components of the Council's Our Manchester and Our People strategies have underpinned the policy content to enable and empower our workforce and services. The policy also confirms the Council's position on the use of employees' own ICT equipment to access Council systems.

## Recommendations

The Committee is asked to approve the adoption of the revised Internet and Email policy appended to this report (Appendix A).

---

**Wards affected:** All

**Financial considerations – Revenue:**
None

**Financial considerations – Capital:**
None

---

## Contact Officers:

Name: Lynne Ridsdale
Position: Director of HROD
Telephone: 0161 600 8380
Email: l.ridsdale@manchester.gov.uk

Name: Sam McVaigh
Position: Head of Organisation Development
Telephone: 0161 234 3976
Email: s.mcvaigh@manchester.gov.uk

Name: Nick Morgan
Position: HROD Specialist - Policy Team
Telephone: 0161 234 4090
Email: n.morgan1@manchester.gov.uk

**Background documents (available for public inspection):**

The following documents disclose important facts on which the report is based and have been relied upon in preparing the report. Copies of the background documents are available up to 4 years after the date of the meeting. If you would like a copy please contact one of the contact officers listed on the previous page.

- Report to Personnel Committee, 02 March 2016: *Internet and Email policy*
- Report to Personnel Committee, 03 September 2014: *Social Media Policy*
- Report to Personnel Committee, 03 September 2014: *Social Media Code of Conduct*
- *Information Security Standards (Code of Practice for Information Security*) approved February 2017

**Implications for:**

| **Anti Poverty** | **Equal Opportunities** | **Environment** | **Employment** |
|---|---|---|---|
| No | Yes | No | Yes |

## 1.0 Background & Context

1.1 As the technology available to our employees changes in line with the progress of our ICT Strategy, it is important to ensure that our policies are revised to keep pace with this evolution. The current version of our Internet and Email Policy was published in March 2016 and, as with all our policies, we have a responsibility to review this when there are any changes that impact the organisation.

1.2 The Google digital platform, G Suite, launched across the Council in March of this year. G Suite has the potential to enable our employees to work far more flexibly and collaboratively than ever before. To ensure we are able to support this and protect the organisation, our employees and customers, a revision of the current policy on Internet and Email is required.

1.3 The Our Manchester strategy asks us to *'continue to seek creative and innovative approaches through working collaboratively with others'*. This is underpinned by Our People strategy commitment to the Our Manchester behaviours of working together and trusting each other, 'owning it;' and not being afraid to try new things. The revised Internet and Email policy offers an opportunity to take a positive step towards this through more flexible working in light of technological advances whilst continuing to mitigate any associated risks. In addition to incorporating new technology the revised policy also seeks to support the organisation in facilitating new ways of working and the move towards a fully connected workforce. To support and enable these behaviours it is important that our policy addresses the ways that employees might want to access our systems (both now and in the future) and provides scope for services to try out new ways of delivering their work.

1.4 The Council's proposed Internet and Email policy content has been benchmarked against other local authorities who have migrated to G Suite. Alongside this exercise careful consideration was given to the Council's individual requirements ensuring that the policy works for the organisation and our employees.

## 2.0 Policy Content

2.1 This policy aims to ensure all staff are using technology safely, securely and productively. An important part of this is making sure everyone can understand the policy. All sections are written in line with plain English principles and the approach is underpinned by the 'Our Manchester' and 'Our People' strategies.

2.2 Those with access to Council technology are expected to use the systems responsibly and with common sense. To ensure that this is clear the policy includes a section dedicated to responsibilities for all users and for managers. For those who abuse their access privileges, the policy is clear that appropriate management action will be taken.

2.3 Feedback received from across the organisation following the roll-out of G Suite has been considered and incorporated into the revised policy which has

been written by HR & OD staff in collaboration with Audit, Legal and ICT colleagues.

2.4 The revised policy incorporates:

- explicit references to Google where required (for example “Hangouts”)
- a review and appropriate rewording of all sections to ensure the policy is accessible to everyone in the organisation
- embedded links for further information (e.g. associated policies) rather than long appendices
- clearer and condensed responsibilities for all users and managers.

2.5 The section on Information Security (and the policy as a whole) has been written in line with the General Data Protection Regulations (GDPR) currently in effect and which requires compliance by the Council from May 2018. The importance of information governance is highlighted throughout the policy (e.g. managers ensuring their team know how to recognise and report a data breach) as this will be an integral part of our strategy to demonstrate compliance with GDPR.

2.6 The policy sets out the standards that are required when using technology and the measures that will be taken if these are not upheld. It makes employees aware of the security and legal risks with the aim of ensuring all employees are using technology effectively and productively.

2.8 Currently around 1,500 employees do not have access to Council ICT systems. A significant programme of work is currently progressing to provide universal access to all employees. As staff gain access to ICT systems as part of this programme special attention will be given to explaining this policy.

2.9 In the light of the opportunities made available through G Suite it is recognised that the enabling staff to access Council systems through their own devices (e.g.laptops, PCs and smartphones) may have significant benefits both in terms of employee engagement and productivity and is a common feature in most modern organisations. Many employees will already be accessing systems remotely (e.g. at home) through the existing Citrix Access Gateway (CAG) and the policy provides guidance on the organisation’s position on the use of staff-owned devices to access Council systems, ensuring appropriate security measures are in place to maximise the benefits and minimise the risks.

## 3.0 Key Policies and Considerations

### (a) Equal Opportunities

None. In keeping with our current approach support will be offered to employees who require assistive technology to access our ICT systems.

### (b) Risk Management

Further guidance/revisions may be required once G Suite has had further time to embed. The policy will therefore be kept under close review. The revised Internet and Email Policy is a step towards ensuring all our policies are clear and provide compliance with the new data protection regulations. Further policy revisions may be required as the project to comply with GDPR developments.

HROD will continue to work closely with services to ensure that the policy and associated guidance continue to support the requirements of the organisation.

**(c) Legal Considerations**

The key two legal considerations in relation to this policy are employees using technology inappropriately and data breaches. The policy covers these in clear and direct language and will be underpinned by training and induction to instill the responsibilities all our employees have to protect Council systems and information and that of their colleagues and service users.

## 4.0 Trade Union Comments

To follow

## 5.0 Comments of the Director of HROD

5.1 The proposed updated intranet and email policy has been developed to ensure the organisation maximises the benefits available through technological advances whilst continuing to protect the organisation, its staff and service users. The policy provides a positive step forwards in support of our more effective use of technology as an organisation and, in particular, through confirming the Council's position on the use of employee owned devices will support work towards enabling universal ICT access for all staff.

**Appendix A: Intranet & Email Policy**

# Internet and Email policy

**Issued by:**
**HR/OD**
**August 2017**

# Document Control

| | |
|---|---|
| Title | Internet and Email policy |
| Document Type | Policy |
| Author/Owner | HR/OD |
| Subject | Use of Internet and Email |
| Created Date | August 2015 (reviewed May 2017) |
| Approval Date | March 2016 (revised version September 2017) |
| Approval By | Personnel Committee |
| Review due | September 2020 (or earlier where there is a change in the applicable law or an organisation which affects this Policy). |

# 1 Introduction

The use of technology, data and systems forms a large part of our work and we need everyone to use it sensibly and safely. There is a level of trust given to those with access to these systems and, in return, high standards of integrity are expected from everyone using Council technology. This policy sets out what's expected when using this technology and how we can help to protect our information to reduce the risk to both individuals, and the Council.

# 2 Scope

This policy applies to those who have access to Council technology (e.g. internet/email/intranet) and forms part of the induction for new starters and those moving between roles. The policy needs to be read along with the Social Media Policy and Social Media Code of Practice and relevant ICT policies.

# 3 Aims

This policy aims to make sure we are all using technology safely and productively, to achieve this the policy seeks to ensure that:

- the standards for using the internet and email are established and enforced
- those using Council technology are aware of the security and legal risks
- our systems and information are protected, and
- we are using technology effectively and positively.

# 4 Monitoring

## Overview

The use of the internet and email is monitored to help protect our systems and prevent the misuse of technology. For example:

- To protect the email network we scan all our messages for viruses/malware, you may get emails returned if they are sent to an address or contain content that is suspicious.
- All website visits are recorded, on request ICT will provide reports regarding the use of technology to the relevant senior manager.

Any suspected instances of misuse highlighted by these measures will be investigated in accordance with the Council's disciplinary procedures.

### Storage

All communications (e.g. Gmail, Hangouts) are saved in an archive at the time they are sent/received. Communications that are deleted remain in the archive, this means they can still be accessed even if they are deleted from your account.

As a result of the archive all communications can be retrieved for internal investigations and are potentially disclosable under subject access related legislation and court proceedings. This underlines the importance of ensuring that appropriate language and professional care is used in all communications.

Further information on the retention and disposal of business records is available on the Democratic Services (Legal) Intranet pages.

## 5 Intranet, Internet, Email and Instant Messaging

### Intranet

Intranet access is not limited as most of the content relates to the Council. It contains a lot of information and, although we promote its use, it is unacceptable to spend an excessive amount of time browsing content unnecessarily and could lead to disciplinary action as detailed in section 10 Sanctions.

### Internet

Internet use is encouraged for business use and you are trusted not to abuse the access you have (examples of unacceptable use can be found in Appendix A). There is no time limit on internet use as we understand you may need to spend a certain amount of time online as part of your role. However, you may need to explain your use if this seems excessive.

Many sites that could be useful for work require registration, if you want to register on a site for work reasons you should check with your manager first. Some sites will be blocked for security reasons, if you have any problems relating to access contact servicedesk@manchester.gov.uk

### Email

When sending emails the language you use should be professional and sent in line with the ICT guidance on Using Email securely. As good practice, time critical and important business external emails (e.g. tender requests, contracts) should be followed up to make sure they have arrived.

When you are sending an email:

- Remember to check the address you are sending the email to is correct (especially with confidential/sensitive information).
- When sending group emails or when selecting ‘Reply to all’ it is your responsibility to make sure that everyone listed needs to see the information you are sending.

- External email is vulnerable as it passes over the internet. As the security of these emails cannot be guaranteed, encryption must be used for transmitting confidential data.

Only open files and links from emails where the source is trusted. If you receive something you are not sure of please forward the whole email to internet.administrators@manchester.gov.uk and then delete.

All work-related emails should have a signature which includes your name, job title, and contact details.

### *Requesting access to an email account*

Managers can ask for and should be granted access to their team's email accounts, for example to check emails when a member of the team is absent from work unexpectedly.

Additionally access to emails including those labelled 'PERSONAL' may take place when unauthorised activity is suspected. If we need to access your emails/files the relevant authorisation will be sought, and you should usually be informed and given the reason why.

### *Sharing access*

You may be asked to grant access to your emails as this can help if you are off unexpectedly and your colleagues need to find information and check your emails.

Managers will periodically remind their team members to remove access previously granted which may no longer be required.

Your login details must not be shared. Those requiring access to a specific ICT system can 'request a service' via the ICT intranet page.

### *Personal use of email*

Although our email system is for business use we understand that you may, on occasion, need to use your work account for personal emails. Limited personal use is allowed on the basis that the guidelines detailed in Appendix B (Personal use of internet and email) are followed.

### Messaging (Google Hangouts)

It may be less formal but the same standards are expected when using Hangouts. These messages will be archived and any misuse will be investigated in the same way as if you were sending emails, this could lead to Hangouts being disabled on your account and disciplinary action being taken.

## 6 Using Personal Devices

Not everyone needs a Council mobile device (e.g. work mobile phone or tablet) as part of their role. We understand that some staff may choose to, on occasion, access Council systems (e.g. email) from their own devices such as laptops/PCs or smartphones.

This is acceptable as long as you are sensible and do not put the integrity of Council systems at risk:

- When accessing Council systems (on any device) your conduct and usage should be in line with the relevant Council policies and guidance such as Protecting Information and the Employee Code of Conduct.
- Your Gmail account must have two step verification turned on.
- Do not select 'keep me signed in' when logging into G Suite using a personal device.
- Do not download and store any content from your Council account (e.g. documents) on your personal device.
- Anti-virus protection must be installed and kept up to date on any device that is used for remote access.

It is recommended that employees register their mobile devices which they wish to use in order to access Council systems for Mobile Device Management (MDM). This provides a secure area on the device for you to access Council systems which is separate to any of your personal information/apps etc and provides a greater level of protection for Council information. Contact the ICT service desk for more information.

# 7 Information Security

The Council has a duty to ensure the confidential information it holds is protected. Complying with this policy will minimise the risk of breaching this duty, whilst also preventing misuse of the email and internet/intranet facilities.

Under the General Data Protection Regulation (GDPR) you are directly responsible for meeting the obligation to protect any personal data transferred about an individual. The Data Protection Principles outline our responsibilities in relation to the Act and further information can be found in the Democratic Services (Legal) intranet page.

Everyone using Council technology should become familiar with The Information Security Code of Practice which provides guidance on the secure use of email and the internet. Any misuse of your work email or internet access which breaches the requirement of this policy, or the Information Security Code of Practice, could lead to formal action under civil or criminal law and/or under the Council's disciplinary procedure.

## Key considerations for maintaining information security:

- We all need to follow the 12 Golden Rules around using ICT and protecting information.
- Instructions regarding the use of technology from the ICT service and your manager must be followed.
- If you use Council technology remotely (e.g. from home), security needs to be in place so Council information is protected.
- Only those authorised should be able to access Council technology on your devices (laptop/mobile etc), these must be kept secure to prevent loss or theft.
- Nothing relating to work should be sent to personal email addresses (unless this forms part of your role and you have authorisation from your manager).
- Information shared via Council technology should only be for business purposes.

- Confidential emails should be sent using encryption software and/or secure email accounts.

Further detail on the steps we need to take to comply with the law on information and technology can be found in the Information Security Policy on the ICT intranet pages.

### *Passwords*

Following a few simple rules can make it difficult for unauthorised people to gain access to our ICT systems:

- Never reveal your password.
- Never ask anyone else to reveal their password to you.
- Under no circumstances share your password.
- Never write your passwords down.
- Do not use anything that could be easily recognisable as a password. For example, your pet's name.
- Use additional security where possible (such as two step verification).

More information on passwords can be found in the IT Access Control Policy that can be found on the ICT intranet pages.

### *Filtering Software*

To protect the email network communications are scanned by software to identify spam and viruses. The Council uses message monitoring, filtering and rejection systems as appropriate, and this software restricts transmission of messages that may breach the terms of this policy.

Filtering software is also used to prevent access to internet sites which are not work related and which are considered to be inappropriate.

### *Access*

All information (e.g. data/email) sent or received over Council systems for business purposes belongs to the Council, this information forms an integral part of the Council's business records.

# 8 Responsibilities

## All Users

Everyone with access to Council technology is expected to:

- use the Council's ICT facilities responsibly and in accordance with the relevant policies
- understand their responsibilities in relation to the Information Security Code of Practice
- ensure their actions do not compromise the integrity of the Council's ICT systems
- take responsibility for ensuring confidential information is only disclosed lawfully and with appropriate authorisation (see the Protecting Information page for more information)
- report security breaches in line with the Information Security Incident Management Procedure

- inform ICT if they visit a website or receive an email which could be malicious, and
- report any emails received which include unacceptable content.

Above all else we should all use common sense when using Council technology. If you are not sure then just check first.

### Managers

Are responsible for:

- being an example to their team, demonstrating good practice when using technology
- ensuring that their team have an understanding of this policy
- checking their team can recognise and know how to report a data breach, and
- monitoring the extent of personal use to make sure it's not impacting on work.

Managers should also make it clear that a breach of any policy relating to the use of Council technology will be investigated in accordance with the disciplinary policy.

## 9 Public Access to Information Held by the Council

Accounts may be accessed to retrieve information, such access will be limited to the accounts required and we will only retrieve relevant information. Access will be approved by an authorised person before the information is retrieved. The Information Commissioner's Office (ICO) subject access code of practice and the Democratic Services (Legal) intranet site provide further information regarding access to information .

## 10 Sanctions

Failure to observe the requirements of this policy may result in the following action:

- Disciplinary action, up to and including summary dismissal being taken under the Council's disciplinary procedure.
- The rescinding of access to the internet and other technology and, where applicable, civil action and/or criminal charges.

Any authorised user who breaches this policy, who is not employed by, or under the direct control of the Council will be liable to any other sanctions the business relationship or law permits.

Where the use of data and/or technology potentially breaches civil and criminal law, the City Solicitor will be informed.

## 11 Declaration

When you log on for the first time (and periodically after that) you will be required to accept that you have read, understand and agree to the terms of this policy.

Those who fail to confirm their agreement may have their access suspended.

# 12 Legal considerations

This policy has been written in line with the following legislation:

Computer Misuse Act 1990
Data Protection Act 1998 (General Data Protection Regulation 2016)
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Telecommunications Regulations 2000

# Appendix A: Examples of unacceptable use

The following points are some examples of internet and email use which would be unacceptable and could constitute gross misconduct:

- Setting up or maintaining websites, web based email or instant messaging accounts for personal use
- Participating in chat rooms, forums or social media for reasons other than business purposes
- Accessing auction sites, for example eBay for reasons other than business purposes
- Streaming or downloading content which is not work related
- Gaining unauthorised access to systems
- Bringing the Council into disrepute, breaching any policy of the Council or its objectives or values
- Operating or managing any private business, commercial/profit making activities and/or activity for personal financial gain
- Sending emails that consist of unsolicited material, promotional or advertising material, including initiating or continuing chain emails
- Wasting staff effort or resources or causing disruption to the Council's communication systems
- Sending emails that are designed, by intent or otherwise, to cause annoyance, offence, inconvenience or anxiety
- To knowingly expose the system to viruses and/or junk mail/spam
- Infringe the copyright of another person, including intellectual property rights
- Accessing, downloading, sending or storing text, images or other material which could be considered discriminatory, offensive or illegal
- Disclosing confidential or commercially sensitive information regarding the Council's activities or personal information about service users or employees.
- Sending emails that violate the privacy of others, unfairly criticise or misrepresent others, or claim to come from an individual other than the user actually sending the message.

The above is not an exhaustive list, it serves to provide examples of unacceptable use which could lead to disciplinary action and, ultimately, result in dismissal.

# Appendix B: Personal use of internet and email

A limited amount of personal use is allowed. However, this is a privilege, not an entitlement, and is permitted on condition that this use does not:

- Impact on the individual's work performance or service delivery.
- Involve the private buying or selling of any goods or services
- Involve using your Council email address to subscribe to non-work related mailing lists
- Take priority or interfere with the performance of the your duties or those of your colleagues
- Cause any expense or liability to be incurred by the Council
- Include any work related attachments, documents, links etc
- Conflict with the Council's objectives, values or have an adverse impact on the role of the Council in any way.

Personal use outside these conditions may be allowed under exceptional circumstances. Always speak to your manager first to let them know you want to use your work account for personal use.

*Sending personal emails*

There is very limited privacy when sending personal emails, these can still be accessed if required. When sending personal emails you must ensure:

- All emails are marked 'PERSONAL' in the subject header
- All emails sent or received must be labelled as 'PERSONAL'
- You inform anyone outside of the Council, who is sending you a private message to identify the message as 'PERSONAL' in the email header; and
- Your signature (i.e. job title, location, contact details etc) should be removed from all emails sent.

All emails that are not marked 'PERSONAL', will be deemed to be business communications.

If you need to send sensitive information, for example to Occupational Health or your Trade Union, consider alternatives to email.

Remember, even when you delete personal emails these may be captured and stored for a defined period in the archives, this also applies to communications via Hangouts.

Further guidance on good practice is available on the ICT intranet pages.