Digital Media Policy

1. Introduction

1.1 This policy provides a single document for staff which addresses how they should approach all forms of digital media, both in their working and personal lives. For the purposes of this policy any form of media that can be viewed on digital devices such as computers, tablets or smartphones will be regarded as digital media. This includes but is not limited to:

- Email
- Social Media
- The Internet
- The Intranet
- Any integrated social features within the Intranet

1.2 Although there are some sections of this policy that specifically refer to social media or email, the same overarching principles of the Employee Code of Conduct and information security applies to all digital media.

2. Scope

2.1 This policy applies to all Manchester City Council employees, contractors, casual workers and agency workers.

2.2 It outlines the responsibilities and standards expected when using digital media inside and outside work, for both business and personal purposes, which relate to:

- Information Security and Confidentiality
- Authorisation procedure for official Council accounts
- Conduct in both personal and professional use of digital media

2.3 This policy should be read alongside our Information and Cyber Security Policy.

3. Aims

3.1 This policy aims to:

- Give clear guidelines to all staff on the standards of behaviour that are expected in respect of digital media.
- Help staff to be mindful of the balance between their personal and professional digital media use.
- Comply with the law on discrimination and data protection of both users of the service and staff.

- Be clear that the Council's digital media network is monitored (see section 11), and explain how disciplinary rules and sanctions apply to any misuse of digital media.
- Help protect the Council against potential liability for the possible actions of staff.

4. Legal

4.1 The statutory framework relating to this policy is as follows:

- Equality Act 2010
- Defamation Act 1996
- Human Rights Act 1998
- Investigatory Powers Act 2016
- Investigatory Powers (Interception by Businesses etc for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356)
- Data Protection Act 2018
- General Data Protection Regulation (2016/679 EU)

---

5. Policy Provisions and Principles of Use

5.1 Staff are expected to treat colleagues, partners and customers with the respect that they deserve. As such, all use of digital media should be in accordance with the behaviours within the Employee Code of Conduct. Any member of staff that is responsible for inappropriate or offensive activity on digital media may be subject to the Council's agreed disciplinary procedure. Examples of unacceptable conduct include:

- Abusive or threatening behaviour
- Inappropriate comments or material that may be regarded as discriminatory
- False or misleading statements that could have a negative impact on our reputation
- Inciting or supporting somebody to commit a crime or other unlawful act

5.2 This could include content that is posted, shared, or 'liked'.

5.3 The Council's response to any reported misuse of social media will be reasonable and proportionate to the perceived offence, the nature and context of the material, and the impact or potential impact on the Council.

5.4 Even if a member of staff does not identify as Council staff, this policy will still apply if a connection with their employment can be made. Staff should be mindful that they are responsible for their words and actions in an online environment, and unacceptable conduct may result in disciplinary action.

5.5 Digital media must not be used to raise or discuss a complaint or grievance about the Council, a manager, or colleagues. Any complaint should be raised through the Council's Employee Dispute Resolution procedures. In most cases concerns should be raised with the appropriate line manager, however if this is not possible then the Council's Whistleblowing Policy may be applicable.

5.6 Under no circumstances must a member of staff share confidential information arising from their employment with the Council, including - but not restricted to - the following:

- information about service users
- information that is politically or commercially sensitive
- any information intended for internal use only (including matters concerning council services, organisational change or related proposals)
- intellectual property

Information Security

5.7 The Council has a duty to ensure that the confidential information it holds is protected, and under the General Data Protection Regulation (GDPR) staff are responsible for meeting the obligation to protect any personal data relating to individuals.

5.8 Everyone using digital media should be familiar with the 12 Golden Rules and Cyber Security best practice.

Cyber Bullying

5.9 Cyber bullying is any form of bullying which takes place online. The Council regards cyber-bullying as seriously as any other form of bullying or harassment. If staff have an issue about behaviour at work, then this should be discussed with an appropriate manager.

---

6. Roles and Responsibilities

6.1 Line managers are responsible for:

- Ensuring that their team have an understanding of this policy
- Checking that their team can recognise and report a data breach
- Ensuring that account moderators and any social media accounts within their control are monitored effectively and operate within this Policy.
- Informing the Strategic Communications Team about any changes to the management of accounts, including change of account moderators and passwords.

6.2 On receiving access to social media, all account moderators will be asked to sign a declaration and affirm their acceptance of the principles of the Digital Media Policy. Failure to acknowledge acceptance of these principles will result in access to social media facilities being denied.

6.3 All staff are responsible for:

- Ensuring that their use of digital media (as defined in para 1.1) is in line with this policy.
- Understand their responsibilities in relation to the Information and Cyber Security Policy (see para 5.8) and the protection of confidential information (see para 5.7).
- Reporting any security breaches in line with the Information Security Incident Management Procedure.

6.4 The Strategic Communications Team are responsible for approving Council social media accounts, and will maintain a record of all accounts, their moderators and passwords. They will support the initial development of Council accounts and monitor accounts using a social media monitoring application; they will also be responsible for advising on the appropriate use of digital media.

6.5 HROD are responsible for advising and supporting managers on any breaches of this Policy, and any resulting use of formal action such as the Disciplinary Policy.

---

7. Email

7.1 Email remains a fundamental part of how the Council communicates. Staff must be mindful that external email can be more vulnerable than internal email, as it passes over the internet. Encryption must be used when sending confidential information to an external source.

7.2 When sending group emails or when selecting 'Reply to all', it is important to make sure that everyone listed needs to see the information that is being sent. Staff should exercise care not to copy emails automatically to all those copied into the original message to which they are replying. Doing so may result in disclosure of confidential information to the wrong person.

7.3 Legitimate emails and communications should never ask for a username and password. Any suspicious activity must be reported immediately to the ICT Service Desk, or our Cyber Security Team.

7.4 Emails that staff intend to send should be checked carefully. The use of email to send or forward inappropriate messages will be treated as misconduct under the Council's agreed disciplinary procedure.

7.5 Staff should be mindful that their emails will be disclosable in a Freedom of Information or Subject Access Request.

7.6 Statements to avoid in emails include unnecessary criticism of others, those stating that there are quality problems with goods or services of suppliers or customers, and those stating that anyone is incompetent. Staff must also ensure that they do not send untrue statements about others in emails as the organisation could face legal action for libel and be liable for damages.

Email Access

7.7 If a role requires the use of email, then managers can ask for and should be granted access to their team's email accounts, in order that work can be accessed if a member of the team is absent. If access is needed to staff email whilst they are absent, then this can be requested through KnowItAll at the ICT Service Desk.

7.8 Where possible, managers will avoid opening staff emails clearly marked as private or personal. However, access to emails including those labelled as personal may take place when unauthorised activity is suspected. Labelling an email as personal will not prevent disclosure in an internal investigation or a Freedom of Information request, for example.

7.9 If access to staff emails/files are needed then the relevant authorisation will be sought, and the member of staff should usually be informed and given the reason why.

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

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

Alternatives to Internal Email

7.12 Although more informal, the same standards of communication and behaviour are expected when using internal messaging platforms such as Microsoft Teams or WhatsApp groups. Messages will be archived and any misuse will be investigated in the same way as if you were sending emails.

Personal Use of Email

7.13 Although our email system is for business use we understand that staff may, on occasion, need to use their work account for personal emails. Limited personal use is allowed on the basis that the guidelines within this policy are followed.

Staff must not use their work email address to register for any services intended for personal use. Examples of this include online banking, streaming services such as Netflix, and auction sites such as ebay.

---

8. Social Media

8.1 Although the Council has official digital media accounts, there are circumstances where it is appropriate for staff to use their personal accounts to engage with communities or events. We recognise that social media is a central aspect of how we communicate with residents, customers, businesses, and partners. However, staff must be aware that digital media is subject to the same business, legislative and accountability standards as written or verbal communication.

8.2 Any real or apparent conflict of interest should be avoided. As such, staff should take great care before accepting 'friend requests' on social media from service users or their families, contractors, or elected members. Although it is acknowledged that on some applications staff have no control over who chooses to follow them.

8.3 Staff whose work contains elements of safeguarding must always have their professional role in mind when operating in the digital world, and should always consider how their behaviour could affect their professional reputation and employment. As such,

anyone who works with children, young people, adults or their families must not make or accept ‘friend requests’ with service users.

Use of Official Council Social Media

8.4 Staff must not set up any Council social media accounts without the agreement of the Strategic Communications Team, and approval from the appropriate Head of Service.

8.5 Officers with responsibility for Council social media accounts, known as account moderators, must inform the Strategic Communications Team of any changes to account passwords or account moderation.

8.6 Account moderators must only engage with appropriate accounts linked to the Council’s day-to-day business, and not personal interests.

8.7 All Council accounts must have clear Council branding approved by the Strategic Communications Team.

8.8 Account moderators who publish on Council social media accounts are indemnified for posts as long as they have received instructions or information and acted in good faith. The moderator needs to ensure the accuracy of the information, or to ensure that the person asking for the information to be published is authorised to do so.

8.9 Account moderators must regularly review the Council accounts they are responsible for. Any inappropriate content must be removed immediately, and the account moderator must report the content to their line manager, the Strategic Communication Team, and the social media site or application.

8.10 Account moderators must configure social media accounts to encrypt sessions whenever possible. This is extremely important for roaming users who connect via public wi-fi networks.

8.11 Moderators must not:

- Copy content from elsewhere for which The Council does not own copyright.
- Engage in spamming (publishing the same or similar content repeatedly or in bulk).
- Use accounts for any political purposes.
- Endorse or post promotional content for commercial organisations without Head of Service approval.
- Bring the Council into disrepute.

Personal Use of Social Media

Personal Use of Social Media at Work

8.12 The Council encourages staff to make reasonable and appropriate use of digital media as part of their work. It is an important part of how the organisation communicates.

8.13 Staff may use personal social media to engage in the Council's social media activities, for example, by contributing to an official Council Twitter account.

8.14 Staff must always be aware that, while contributing to the Council's social media activities, they are a representative of the Council. If staff choose to comment or post opinions online, regardless of whether or not they hold a politically restricted post, they should take care that their opinions are not perceived as comments made on behalf of the Council, and that they do not bring the Council into disrepute.

Personal Use of Social Media Outside of Work

8.15 The Council recognises that many members of staff make use of social media in a personal capacity. While they are not acting on behalf of the Council, staff must be aware that they can cause reputational damage to the Council if they are recognised as a member of staff.

8.16 If staff do discuss their work on social media (for example, giving opinions on their specialism or the area in which they work), they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer." However, staff should be aware that such a disclaimer will offer no protection from the consequences of unacceptable online conduct. Staff are responsible for anything that they say online.

8.17 When staff are using social media, whether or not they have identified themselves as having an association with the Council, they are expected to behave appropriately at all times and in a manner that is consistent with the Council's values and policies. If a complaint is made then staff may be subject to disciplinary action. Examples of unacceptable online conduct include but are not limited to:

- Abusive or threatening behaviour
- Inappropriate comments or material that may be regarded as discriminatory
- False or misleading statements that could have a negative impact on the Council's reputation
- Disclosure of confidential information relating to service users, colleagues or the business of the Council
- Inciting or supporting somebody to commit a crime or other unlawful act

---

9. The Internet

9.1 Use of the internet is encouraged for business purposes where appropriate. Staff are expected to use it sensibly and in such a manner that it does not interfere with their work.

9.2 The Council also understands that staff may on occasion need to use the internet for personal purposes during work time, although such usage should be kept to a minimum.

9.3 The internet must not be used to access offensive or illegal material. If the online activity of any member of staff is suspected of being in breach of the Employee Code of Conduct, then they may be subject to disciplinary action.

---

10. If a Mistake is Made

10.1 If a member of staff posts something on digital media that they did not mean to, or accidentally sends or posts a badly-worded message, they should tell their line manager and the Strategic Communications Team immediately to agree on any action that may be needed to minimise embarrassment and reputational damage.

10.2 If confidential information is accidentally shared, and a data breach occurs, then this must be reported immediately to the appropriate line manager.

10.3 If a device that is used to access Council social media accounts is lost or stolen, the incident must be reported as soon as possible to the ICT Service Desk.

11. Monitoring

11.1 The Council deploys technical controls to monitor and report on staff use of social media through the Council network. The Council also uses a social media monitoring application to monitor and report all mentions of the Council in social media web spaces.

11.2 To protect the email network all messages are scanned for viruses/malware, and emails may be returned if they are sent to an address or contain content that is suspicious.

11.3 All website visits are recorded, and on request ICT will provide reports regarding the use of technology to the relevant senior manager.

11.4 Any suspected instances of misuse highlighted by these measures will be investigated to establish if there has been a breach of this policy.

12. Enforcement

12.1 Breach of this policy may lead to formal action under the Council's agreed disciplinary procedure up to and including (in serious cases) dismissal, and where applicable may result in civil action and/or criminal charges.

Document Control			
Date effective from		Owner	HR Policy, HROD
Approval date		Approval By	Personnel Committee
Review date			
Three years from the date of approval (or earlier where there is a change in applicable Law)			