DE MONTFORT UNIVERSITY LEICESTER

Human Resources

People and Organisational Development

Policy on the use of email, internet and social media

November 2012
Revised May 2016

Contents

1 Introduction

1.1 De Montfort University recognises the benefits of email, internet and social media and encourages staff to make effective use of these resources both at home and at work.

1.2 This policy helps ensure that staff use these resources effectively and appropriately by setting out expected standards of behaviour in relation to the use of email, the internet and social media to:

- Provide a framework to encourage staff to make appropriate and effective use of electronic resources within a work context.
- Protect both staff and the university from the potential risks associated with the use of email, internet and social media.
- Ensure compliance with the law, particularly in relation to discrimination, data protection and health and safety.
- Set standards of good housekeeping in relation to the proper use and storage of electronic communications.
- Ensure clarity on the university's policy on monitoring of staff use of email and the internet.
- Ensure clarity on how breaches of the policy will be dealt with.

2 Scope

2.1 This policy applies to all staff of De Montfort University. It applies where staff are using email or the internet in connection with their work for the university, whether within or outside of working hours, and whether or not using university owned or supplied facilities or devices eg smart phones, tablets and iPads.

2.2 Personal online activity is not intended to be covered by the scope of this policy. However, staff members should be aware that their personal online activity may come within the scope of the policy if misconduct in breach of this policy occurs and the DMU staff member is identified. Personal use/online activity may therefore come within the scope of this policy regardless of whether or not the activity is undertaken in the staff member's own time and/or using their own resources/equipment.

2.3 The principles of freedom of expression and academic freedom apply to the use of electronic and social media; however, the university requires responsible and legal use of the technologies and facilities available to staff. (See also the university's **Freedom of expression and academic freedom** policy).

2.4 This policy is not intended to limit or restrict legitimate trade union communications or activity.

2.5 Line managers will ensure that self-employed contractors, agency workers or any other individuals working temporarily in the university are made aware of the policy.

3 Benefits and risks

3.1 The evolving use of different forms of electronic communications and media has

a range of benefits for individuals and the university. The potential benefits are numerous and include increased access to academic resources, increased flexibility and promotion of work/life balance, improved communications, better information and knowledge sharing amongst teams and individuals, less bureaucracy, faster response times, and more sustainable working practices. The university increasingly uses multi-media approaches to attract, engage and communicate with current and prospective students, staff, partner organisations or other stakeholders and to promote DMU's brand and raise its profile.

3.2 However, staff should be aware that their email and internet activities may have adverse consequences either for themselves or for the university. These adverse consequences may include lost productivity, risks of 'information-overload', over-reliance on electronic as opposed to face-to-face communications, reputational damage to the university and to individuals (including where applicable to their professional registration), and potential breaches of the law.

4 Breach of the policy

4.1 If a staff member is found to have acted in breach of this policy this may lead to suspension of their access to university-owned email and internet facilities, and/or disciplinary action being taken against them, up to and including dismissal. Separate investigations from professional bodies approving registration may also occur outside the university.

4.2 Any individual suspected of committing a breach of this policy will be required to cooperate with any investigation in accordance with the disciplinary procedure.

4.3 An individual may be required to remove internet or social media posts that are found by the university to be in breach of the policy. Failure to comply with such a request may in itself result in disciplinary action, up to and including dismissal. In addition staff members may face legal proceedings if comments posted about the university or named individuals are found to have harmed its/their reputation.

4.4 Some examples of unacceptable use and/or potential breaches of the policy are listed below.

- Damaging working relationships between members of staff, students, suppliers and clients of the university, for example, by sending, forwarding or posting messages which are libellous, defamatory, obscene, or in breach of the university's policies such as Data Protection, Code of Conduct, Dignity At Work, or are otherwise inappropriate. This includes posting links to inappropriate content.

- Breaching confidentiality: for example by revealing trade secrets or information owned by the university; giving away confidential information about an individual or organisation; divulging personal data (eg details of salaries, political/religious beliefs, medical information, disciplinary records); or discussing the university's internal workings such as deals or proposed undertakings that have not been communicated to the public, including commercially sensitive information. (If staff members are unsure of what constitutes confidential information they must seek advice from their manager.)

- Breaching the university's IT policies for example, breaches of network security, or downloading and installing unauthorised files or software to the university's network.

- Breaching copyright, for example by using someone else's images or written content without permission, or failing to give acknowledgement where permission has been given to reproduce something.

- Visiting illegal or proscribed websites or downloading or sharing content that is illegal or otherwise obscene including content that is violent or extreme.*

  *If a staff member is engaging in legitimate and university-approved research which requires that person to have access to sites or content that would normally be prohibited by this policy or blocked by the university's servers, including, but not limited to pornography, or the sites of any of the organisations proscribed by the UK government, the university's **Policy on Conducting Sensitive Research** must be followed to protect the university and the staff member from misinterpretation and other adverse consequences for alleged unacceptable use including scrutiny by external law enforcement agencies and possible arrest. See also 7.7.

- Using work email/internet resources for any activities or transactions which are in connection with or support any personal or family business/commercial interest, or which promote personal political or religious views or which in any way implicate or connect the university with such transactions or views except where there is a specific requirement through the staff member's work for the university.

- Using work email/internet resources to set up a chain action (eg chain mail), for 'spamming' or the misuse of mailing lists. (Mass emailing to members of the university eg 'all user' email communications, may be undertaken only where prior approval has been obtained.)

- Excessive personal use of DMU resources that is unjustifiable and constitutes time wasting.

- Otherwise bringing the university into disrepute.

4.5 The above list is not intended to be exhaustive. If a staff member is unsure of whether something they propose to do may be in breach of the university's policy they must seek advice from their manager.

4.6 It should be noted that there are a range of other factors to consider in relation to the use of IT not all of which can be covered by this policy and users should refer to the applicable ITMS or health and safety policies available on the intranet.

5 Use of email and the internet at work

5.1 The university encourages all staff to become familiar with email, IM and the internet and to use them effectively in the efficient performance of their duties.

5.2 Staff are expected to use email, IM and the internet responsibly and in such a

way that it does not interfere with the efficient running of the university or the performance of the staff member's, or their colleagues' duties.

5.3 Staff members may be called upon to justify the amount of time they have spent on the internet or particular sites that they have visited if the university suspects the policy is being breached. (See also Monitoring).

6 Personal use of the university's email and internet systems

6.1 The university provides staff with email and internet facilities for work purposes but understands that, from time to time, staff may need to use these resources for personal reasons and/or during work time eg to send or receive a personal email via their work email.

6.2 Staff members are permitted to use these facilities for personal purposes provided that such use is not excessive and:

- does not in any way breach this policy or interfere with the efficient performance of their duties or their or their colleagues' work outputs.
- does not require the university to provide any additional resources than are provided for work purposes.
- they do not enter into any contracts or commitments in the name of or on behalf of the university.

6.3 Staff members should note that all emails or IM messages sent or received by the university's systems are regarded as the property of De Montfort University. Wherever practicable, staff members should use their personal email account (eg hotmail, gmail) to send or receive non-work-related email communications.

7 Monitoring of email and internet use

7.1 The university monitors the use of its electronic communication systems including the use of its email and internet facilities as necessary to comply with legal obligations or where justifiable for legitimate business purposes. In using the university's facilities and systems, individuals consent to such monitoring.

Email

7.2 The university reserves the right to monitor and check individual staff members' emails / IM messages. In using the university's facilities and systems, individuals consent to such monitoring. The university will, where appropriate, endeavour to inform the affected staff member when this is to happen and the reasons for it. The university considers the following to be valid reasons for checking a staff member's email/IM:

- if the member of staff is absent for any reason and communications must be checked to ensure the smooth running of the university. (See the separate guidelines 'Access to email in the absence of the account holder', Appendix A)
- to investigate suspected unacceptable, prohibited or criminal use of the system or in pursuance of a disciplinary investigation into suspected breach

of this or other university policies/regulations

- if the university reasonably suspects or receives credible information that the staff member is sending or receiving messages that are detrimental to the university

- preventing or detecting emails containing malicious code, viruses or other inappropriate content.

7.3 When monitoring emails, the university will normally confine itself to looking at the address and heading of the emails where this is sufficient for the purposes specified in 7.2. However, where this is not sufficient, the university may need to access the full message content. Staff should mark any personal emails as such and encourage those who send them to do the same. The university will avoid, where possible, opening emails clearly marked as personal or emails that are clearly unrelated to the specific purpose.

7.4 Emails that relate to private communications between a trade union representative and their member, or email folders set up for trade union use will not be accessed without prior consultation with the local branch officers or, in the case of a local trade union official, the regional officer.

Internet

7.5 The university reserves the right to monitor staff members' internet use at work at any time. In using the university's facilities and systems, individuals consent to such monitoring. Monitoring of individual users may occur where the university reasonably suspects that a staff member has been accessing the internet in breach of this or any other university policy.

7.6 The university reserves the right to retain information that it has gathered on staff members' use of the internet. This will normally be for a period not exceeding six months but may be longer where there is an identified business need to retain data for a longer period.

7.7 Access to certain sites from university networks may be automatically blocked by the university's systems eg illegal or proscribed websites or sites containing offensive, obscene, extremist or violent material. Staff with a legitimate need to access a site that has been automatically blocked will need to seek approval from their PVC/Dean or Director or higher, to request access (on a one off or limited time basis depending on the need) via the Director of ITMS. Where access is required for approved research purposes the provisions of the **Policy on Conducting Sensitive Research** will apply.

8 Email and online communications

8.1 DMU staff members should be mindful of their duty to act in good faith and in the interests of the university. Email and online communications should never be used in a way that would breach any of the university's policies, defame the university, fellow staff or students, or damage the reputation of the university. Communication with any such effect may lead to action under the university's disciplinary procedure, up to and including dismissal.

NB This does not apply to genuine concerns or complaints raised in accordance with the university's policies and procedures.

8.2 Email and online communications should be treated like any other form of communication and, as such, what is normally regarded as unacceptable in a non-virtual environment (eg a letter, or face to face discussion) is equally unacceptable in a virtual environment. In particular, if a staff member's DMU email address is being used to send a non-work-related email, they must be mindful of their obligation not to bring the university into disrepute. (See also 'Personal use of the university's email and internet systems)'.

8.3 If a DMU staff member receives a business email in error ie where they are not the intended recipient (excluding 'spam' or 'phishing' type emails), they must immediately notify the sender. If a DMU staff member receives an email that is considered to contain inappropriate content they must notify their manager.

8.4 It should be noted that copies of emails/IM can be requested in response to Freedom of Information Act requests, and in response to subject access requests under the Data Protection Act. Where information is exempt under the Freedom of Information Act 2000, it will not be supplied. Irrelevant information concerning third parties will be redacted in accordance with the Data Protection Act 1998.

9 Social media and online networking

9.1 The university defines social media as websites and applications that allow users to share content and/or take part in online networking. Some examples include Facebook, Twitter, LinkedIn, YouTube, Google+, Instagram, Pinterest, Flickr, Tumblr, Reddit and Snapchat.

9.2 Some staff members may contribute to the university's social media activities as part of their role, for example by writing blogs/managing a Facebook account or running an official Twitter account for the university. Staff should be aware that while contributing to the university's social media activities they are representing the university and should use the same safeguards as they would with any other form of communication about the university in the public sphere.

9.3 DMU social media accounts belong to the university and they must be used at all times in accordance with this policy. User names and passwords for university-owned social media accounts may only be issued, re-set or changed by the Director of Marketing and Communications or their delegate.

9.4 Social media identities, logon IDs and usernames may not use DMU's name or logo without prior approval from the Director of Marketing and Communications.

9.5 Staff members using social media for the dissemination of their research should consult the **Policy on Conducting Sensitive Research** where applicable.

Personal use of social media

9.6 The university respects a staff member's right to a private life. However, the university must also ensure that its interests, confidentiality and its reputation are protected at all times.

9.7 Staff members should be mindful of the immediacy of virtual communications and the fact that, in many cases, their comments/actions can create a

permanent record.

9.8 Where staff members are feeling disgruntled about any work-related matter they are reminded of the proper channels for raising issues internally eg the grievance or whistleblowing procedures, and should avoid ‘knee jerk’ responses on social networking sites, blogs or other online forums. They are also reminded of the Employee Assistance Programme, which is a free and confidential service for all DMU staff members. DMU staff who are members of a trade union may also seek support and advice from their trade union representative.

9.9 Staff members should be aware that social networking websites and blogs are public forums, particularly if the staff member is part of a "network". Even where staff members have restricted their personal privacy settings, they should not assume that their entries on any website or online forum are or will remain private.

Personal websites and blogs

9.10 Where staff members have a personal website or blog, or where they contribute to or post comments on any other form of online discussion/noticeboard/blog, and where they are reasonably identifiable as a DMU staff member, the following will also apply:

- Staff members should state to their readers that the views and opinions that they express are theirs only. They should include a notice such as the following: "The views expressed on this website/blog are mine alone and do not necessarily reflect the views of any other individual or organisation".

- Staff members must not link their site/blog/comments to the university’s website without having complied with the above requirement and without the university’s consent.

- Staff members must not use the university’s logo, website, internet systems or intranet for their personal website or blog.

10 Diversity and exclusion

Staff members should remember that not all DMU colleagues will be able to engage in social networking activity or may prefer not to do so. Where social media/networking sites are used in the work context eg for discussion/debate amongst colleagues, to share information and learning or to arrange team social activities, it is important that colleagues who cannot or choose not to participate in social networking are not excluded or otherwise isolated.

11 Safe working practices

11.1 The increasing use of email, internet and social media in both the work and home setting creates additional risks in relation to safety and wellbeing for staff members and risk assessments eg work station risk assessments, should take into account not only the increased reliance on such working practices, but also issues such as workplace design.

11.2 DMU staff are advised to refer to the relevant health and safety and risk

management policies and processes available on the intranet.

12 Leavers

A staff member's email account and network access will normally cease when the staff member no longer works for the university, unless an agreement has been reached with the university in respect of a period of retention after leaving the university's employment.

13 Communication of the policy and future updates

Technology and the law change regularly and this policy will be updated to account for changes as and when necessary in consultation with the recognised trade unions.

Appendix A: Access to email in the absence of the account holder

1. Staff members may be asked to nominate a colleague to have "read only" access to their email inbox in their absence, where the university deems this to be necessary. The link for this process is https://sites.google.com/a/myapps.dmu.ac.uk/isas/help-support/self-help

2. Where provision has not been made under the process above, and there is a genuine business need to access a staff member's emails in their absence, there are two options available as set out below.

Out of Office Assistant

3. If a staff member is unexpectedly absent a request can be made to activate the "Out of Office Assistant" on the account. The request must be made to the ITMS Service Desk by the staff member's line manager stating:

- name of the absent staff member
- the reason for the request
- the text of the "Out of Office Assistant" message.

4. Notification will be sent to the staff member and their line manager by ITMS that this has been done and it is expected the staff member will deactivate the 'Out of Office Assistant' on their return to work.

Access to a staff member's email account

5. If there is a genuine business need to access a staff member's emails and the individual user has not nominated a colleague, or consented to another colleague having 'read only' access (as per [1] above), the following procedure should be followed:

i. An access request must be made to the ITMS Service Desk itmsservicedesk@dmu.ac.uk by the staff member's line manager stating:

- name of member of staff absent
- length of time access is required for (see 7 below)
- reason for requesting access.

ii. This will be logged as a Service Desk call and passed to People and Organisational Development for approval of the request. Once approved and actioned, notification will be sent to the staff member and their line manager from ITMS that this has been done.

iii. Only emails that appear relevant to the access request will be opened. Emails that are marked 'personal' will not be opened unless there are convincing grounds on which to believe they are in fact relevant to the university's business.

iv. The person granted access will not delete any emails from the staff member's email account.

6. It is not permissible in any circumstances either to request a staff member's username and password, or to request that email is forwarded to an email

account external to DMU.

7. The access provisions will cease once the business need has been addressed and/or it has been possible to make an alternative provision, or the staff member has returned to work.