THE UNIVERSITY of EDINBURGH

Policy on Employee Use of Social Media

1. Policy Statement

The University recognises the benefits that the use of social media can bring to the organisation, and to individual employees, both in their personal and working lives.

Although the University allows employees open access to the internet and email whilst at work, access for personal purposes should be kept to a minimum and should generally be made during permitted breaks from work or outside of work time.

The use of social media to further the interest of and to support the business of the University is encouraged. However, approval should always be sought from managers where such use is proposed.

This policy should be read in conjunction with the University's Computing Regulations, Social Media Guidelines for Staff and Researchers, the University's Data Protection policy and the Dignity and Respect Policy.

2. Scope and Purpose

The policy applies to all employees of the University. It also applies to those people operating on behalf of the University, such as contractors, agency staff and visiting academics. In these situations the Manager responsible for the contractor, visitor or agency member of staff will be responsible for making these staff aware of the University's Policy.

This policy applies to the use of social media for both business and personal purposes, whether it is in normal work time or not, on University or personal computing facilities, and whether posting on social media using personal or work related accounts. It also outlines what the University views as unacceptable use of social media. The Policy does not undermine the principles of academic freedom.

Social media can include, but is not limited to Facebook, Linkedin, Capital I, Twitter, Google+, Wordpress Blogs or Myspace, and is generally identified as web based forums where individuals communicate with friends, family, colleagues, clients or the general public. For the purposes of this policy it also

extends to other personal use of the internet for communication, e.g. blogs, YouTube and non-work email lists.

3. Responsible Use of Social Media

The University has no direct control over the information employees choose to disclose on social networking sites. However, employees must bear in mind the need to protect the reputation of the University, their own privacy, the privacy of colleagues and students and the confidentiality of University information/data in any communications or statements they make available to members of the general public, which includes family and friends outside of the University.

The expectation would be that employees behave professionally in all situations which relate directly or indirectly to the University and should conduct themselves in a way which acknowledges the standards of behaviour expected within this and other University Policies.

If during the course of the investigation a student or member of the public raises a complaint through the University Complaint Handling Procedure (CHP), the Investigating Officer should familiarise themselves with the CHP and seek advice, if necessary.

3.1 Protecting Reputation and Relationships

Regardless of how the information comes to light, an investigation may be undertaken. Disciplinary action may result if following an investigation there is evidence of damage to:

- The reputation of the University
- Working relationships within the University
- Working relationships with external / collaborative partners
- Relationships with students, customers or service providers

At a practical level, all employees are advised to avoid posting anything online that they would not wish managers or colleagues (both internal and external) to see.

3.2 Confidential Information

Employees must not disclose confidential information, or sensitive business related information through Social Media. Additionally, employees must always pay due regard to the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act, and as such ensure that they do not disclose information which could constitute a breach of data protection legislation.

If following an investigation there is evidence of any unauthorised disclosure of confidential information, or action which leads to a potential breach of data protection legislation, this may also lead to disciplinary action for the employee concerned.

3.3 General Guidance on the use of Social Media

Employees should always remember that any information disclosed through personal accounts on social networking sites is disclosed in a personal capacity, and never on behalf of the University.

Where employees disclose their association with the University through Social Media used for personal purposes, any views they publish should be presented as purely personal views rather than being representative of the views of the University.

Employees must also bear in mind their audience when posting on social media sites. They should ensure that those who are able to access the information they post have a right to see it, and also that it is appropriate that they see such information.

If using social media in their capacity as an employee, it is important to ensure that the University's interests are considered, where in doubt advice should be sought in the first instance through the employee's manager.

3.4 Account Security

Employees must always ensure that security information for personal and work related accounts remains confidential, and that they do not disclose log-in information, including passwords, to people who are not authorised to use those accounts.

Where unauthorised access has been gained to an account, there is the possibility of further security breaches and potential damage to personal and/or the University's reputation.

If an employee believes that unauthorised access has been gained to a work related account, they should contact their local IS representative in the first instance for advice.

4. Breaches of this Policy

Social Media should never be used in a way that breaches this Policy, or any other University Policy. If an internet posting, blog or social media comment would breach any of the University's policies in another medium, then it will also breach them in an on-line forum.

For example, employees must not use Social Media in a way that would:

- Breach the Computing Regulations
- Breach the 'Social Media Guidelines for Staff and Researchers'
- Breach any obligations in relation to confidentiality
- Defame the University, or its affiliates, students, staff, suppliers or other stakeholders
- Harass or bully any employee, student or third party or breach the Dignity and Respect Policy
- Unlawfully discriminate against other employees, students or third parties
- Breach the Data Protection Policy.

Where an employee identifies a potential breach of this policy, they should in the first instance report the matter to their manager who should seek advice from their College / Professional Services Group HR Advisor. Employees have the right to raise a Grievance where they believe a colleague has inappropriately disclosed personal information about them, or information which they believe may negatively affect working relationships. They may also refer to the University's Dignity and Respect Policy for further guidance and information, and discuss the matter with a Dignity and Respect Adviser if they require further support.

Managers identifying breaches of the policy should again refer to their HR Advisor in the first instance.

5. Useful Links

The University's Computing Regulations: https://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/computing-regulations

Social Media Guidelines for Staff and Researchers: https://www.ed.ac.uk/files/atoms/files/111201_uoe-social-media-guidelines_0.pdf

The Disciplinary Policy: A to Z of HR Policies | The University of Edinburgh

Dignity and Respect Policy: A to Z of HR Policies | The University of Edinburgh

The University's Data Protection Policy: https://www.ed.ac.uk/records-management/policy/data-protection

6. Policy History and Review

This policy was approved by CJCNC on 27 September 2013 and takes effect from that date. It was updated in March 2021 to include reference to the General Data Protection Regulation and minor changes to organisational terminology.

In the event of any significant change to legislation associated with, or affecting employee use of Social Media, this policy will be subject to immediate review.

In the absence of such a change, the policy will be reviewed by December 2021.

7. Alternative Formats

If you require this document in an alternative format please email UHRS@ed.ac.uk or telephone 0131 650 8127.