

1. Aims & Objectives

- 1.1 This Policy aims to outline the responsibilities of employees, trustees and affiliated student groups when utilising social media, either in a personal capacity or for Association purposes; it also aims to manage organisational risks when social media is used for both business and personal use, and to ensure that use of social media is acceptable and avoids bringing the Association into disrepute.

2. Definitions

- 2.1 “Social media”, for the purposes of this policy, refers to online tools, websites and interactive media that enable users to share information, knowledge, opinions and interests through the use of online communities and networks, encouraging participation, dialogue and involvement. Social media sites include, but are not limited to, Facebook, Twitter, Google+, Instagram, Pinterest, Foursquare and LinkedIn, plus countless online forums.
- 2.2 “Affiliated student groups” refers to all student groups, societies, clubs or committees registered with the Association and eligible to receive staff support and other resources under Association rules. This definition includes USSA Clubs & Societies, Sports Clubs, liberation groups and media groups, and applies whether or not direct funding is received from the Association for the day-to-day running of that group.

3. Scope

- 3.1 This policy applies to all employees and trustees of the Association, and affiliated student groups.
- 3.2 While the Association recognises the value that social media provides if used in a responsible and professional manner, it is also recognised that individuals are personally accountable for their behaviour, and may be held responsible for any breaches of this policy.

4. Legislation

- 4.1 The Association will adhere to its obligations under legislation relevant to the use and monitoring of electronic communication, which are predominantly the Regulation of Investigatory Powers Act 2000; the Communications Act 2003; the Data Protection Act 1998; the Human Rights Act 1998; The Defamation Act 1996; and the Equality Act 2010.
- 4.2 In order to mitigate against the potential risk of defamation and libel claims, pages encouraging discussion should always contain a User Guide instructing members not to use

abusive terms, rather encouraging them to discuss issues in a manner that does not attack individuals.

5. Data Protection & Monitoring

5.1 Whilst computers used within Association buildings are property of the Association, and are primarily intended to assist in the performance of Association business, the Association's IT provision and support falls under the auspices of the University of Strathclyde.

5.2 Usage of Association IT equipment is monitored under the University's Information Security Policy:

<http://www.strath.ac.uk/staff/policies/informationsecurity/>

5.3 The University's Information Security Policy applies to all students at Strathclyde through the Registration process.

6. Privacy Settings & Personal Information

6.1 Default privacy settings for some social media websites allow some information to be shared beyond an individual's contacts. In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. Information available on social media sites could be produced as evidence by the Association, Association staff, Association trustees or affiliated student groups, should it be necessary either as part of Association procedures, or in legal proceedings.

6.2 It is therefore vital that employees, trustees and affiliated groups are strongly encouraged to review their access and privacy settings for any social media sites in order to control and restrict who can access information on these sites; even if privacy and security settings are utilised, anything posted on social media sites may be made public by onward transmission.

6.3 To avoid identity theft, employees, trustees and affiliated student groups are advised to refrain from publishing any personal or sensitive information on social media websites, eg home address, telephone numbers, or any information related to personal bank accounts.

7. Acceptable Use Of Social Media At Work

7.1 Employees or trustees responsible for contributing to the Association's social media activities should be aware at all times that they are representing the Association.

7.2 The Association's IT systems are first and foremost business tools, and as such personal usage of these systems is a privilege and not a right. Employees and trustees are, however, permitted to make reasonable and appropriate use of social media websites where this is part of the normal duties of their work.

- 7.3 Personal use of social media should not interfere with employees' or trustees' work duties and responsibilities. Excessive personal use of social media during working hours and/or abuse of this Policy will be considered as disciplinary offence.

8. Standards Of Conduct On Social Media Websites

- 8.1 The line between public and private, professional and personal is not always clearly defined when using social media. If an employee or trustee identifies themselves as working for or representing the Association, this has the potential to create perceptions about the Association to a range of external audiences, as well as to students and colleagues.
- 8.2 While using social media in any capacity, employees', trustees' and affiliated student groups' actions can still damage the Association's reputation. As such, it is essential that appropriate conduct is used, and inappropriate conduct avoided, at all times.
- 8.3 For the purposes of clarification, the following are considered essential and appropriate conduct:
- i. Conduct in accordance with this policy and other Association policies and procedures, particularly when using Association social media accounts or links;
 - ii. Be professional, courteous and respectful to others, and act in accordance with the Association's Values at all times;
 - iii. Remove or request the removal of any inappropriate comments, images or videos
- 8.4 Examples of inappropriate conduct include (but are not limited to):
- i. Making comments or engaging in behaviour that may be deemed to bring the Association into disrepute;
 - ii. Breaching confidentiality by disclosing privileged, sensitive and/or confidential information;
 - iii. Posting remarks that could be considered to be victimisation, bullying, harassing or discriminatory against any individual or group;
 - iv. Posting or uploading inappropriate images, photographs or video clips;
 - v. Publishing defamatory and/or knowingly false material about the Association, other employees, trustees, members or external organisations;
 - vi. Use of offensive, derogatory or intimidating language which may damage working relationships;

9. Breach Of Policy

- 9.1 Any breach of this policy will be dealt with in accordance with the appropriate Association disciplinary procedure. Disciplinary procedures are contained within the Staff Handbook, Trustee Boards Code Of Conduct and the Association Constitution.
- 9.2 Persistent and/or serious breaches of this policy may lead to dismissal, removal from Trustee Board, or disaffiliation from the Association.