MSU INFORMATION AND COMMUNICATION SYSTEMS POLICY

Clause **Page**

1 Policy statement

1.1 Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor their use, and the action we will take in respect of breaches of these standards.

1.2 In particular, remember that you are representatives of Marjon Student Union and all communication through our systems (whether by telephone, e-mail or otherwise), must be conducted in an appropriate manner.

1.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2 Who is covered by the policy?

2.1 This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as staff in this policy).

2.2 Third parties who have access to our IT and communication systems are also required to comply with this policy.

3 The scope and purpose of the policy

3.1 This policy deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones (including BlackBerrys and other smartphones), personal digital assistants (PDAs) and voicemail. It also applies to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards.

3.2 Misuse of IT and communications systems can damage the business and reputation of MSU.

All staff must comply with this policy at all times to protect our IT and communications systems from unauthorised access, misuse, and harm. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

4 Personnel responsible for implementation of the policy

4.1 Senior Management has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to General Manager Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to our operations also lies with

4.2 The IT Department will deal with requests for permission or assistance under any provisions of this policy, subject to their primary tasks of maintaining our core systems, and may specify certain standards of equipment or procedures to ensure security and compatibility.

4.3 All managers have a specific responsibility to operate within the boundaries of this policy, ensure that all staff understand the standards of behaviour expected of them and to take action when behaviour falls below its requirements. Managers will be given training in order to do so.

4.4 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of our electronic communications systems or equipment should be reported to [the Head of the IT Department. Questions regarding the content or application of this policy should be directed to the Head of the IT Department.

5 Equipment security and passwords

5.1 Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy.

5.2 If given access to the e-mail system or to the internet, staff are responsible for the security of their terminals. If leaving a terminal unattended or on leaving the office they should ensure that they lock their terminal or log off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use terminals under supervision.

5.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the IT Department.

5.4 Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by [**RELEVANT POSITION TBA**]. For the avoidance of doubt, on the termination of employment (for any reason) staff must provide details of their passwords to [**RELEVANT POSITION TBA**] and return any equipment, key fobs or cards.

5.5 Staff who have been issued with a laptop, PDA or Blackberry must ensure that it is kept secure at all times, especially when travelling. Passwords must be

used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

6 Systems and data security

6.1 Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

6.2 Staff should not download or install software from external sources without authorisation from [**APPROPRIATE POSITION TBA**]. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the IT Department before they are downloaded. If in doubt, staff should seek advice from the IT Department. The following must never be accessed from the network: online radio, audio and video streaming, instant messaging and webmail (such as Hotmail or Yahoo) and social networking sites (such as Facebook, Bebo, Second Life, YouTube, Twitter). This list may be modified from time to time.

6.3 No device or equipment should be attached to our systems without the prior approval of the IT Department. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port or any other port.

6.4 We monitor all e-mails passing through our system for viruses. Staff should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .ex). The IT Department should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to e-mails for the purpose of effective use of the system and for compliance with this policy. We also reserve the right not to transmit any e-mail message.

6.5 Staff should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

6.6 Staff using laptops or wi-fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the IT Department from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

7 E-mail etiquette and content

7.1 E-mail is a vital business tool, but an informal means of communication, and should be used with great care and discipline. Staff should always consider if e-mail is the appropriate method for a particular communication. Correspondence with third parties by e-mail should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included. Hard copies of e-mails should be kept on the appropriate file.

7.2 Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling and use an out of office response when away from the office for more than a day. They should endeavour to respond to e-mails marked “high priority” within 24 hours.

7.3 Staff must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform their line manager and/or the Human Resources Department.

7.4 Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should

assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

7.5 E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

7.6 In general, staff should not:

7.6.1 send or forward private e-mails at work which they would not want a third party to read;

7.6.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

7.6.3 contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;

7.6.4 sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

7.6.5 agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;

7.6.6 download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

7.6.7 send messages from another worker's computer or under an assumed name unless specifically authorised; or

7.6.8 send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

7.6.9 Staff who receive a wrongly-delivered e-mail should return it to the sender.

8 Use of the internet

8.1 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in Paragraph 11.2, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature. This is further considered under Inappropriate use of equipment and systems at Paragraph 11.

8.2 Staff should therefore not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy

8.3 Staff should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in their own time.

9 Personal use of systems

9.1 We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not

a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

9.2 The following conditions must be met for personal usage to continue:

9.2.1 use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.30 pm);

9.2.2 personal e-mails must be labelled “personal” in the subject header;

9.2.3 use must not interfere with business or office commitments;

9.2.4 use must not commit us to any marginal costs; and

9.2.5 use must comply with our policies including the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure (see Paragraph 7, E-mail etiquette and content and Paragraph 8, Use of the internet).

9.3 Staff should be aware that personal use of our systems may be monitored (see Paragraph 10) and, where breaches of this policy are found, action may be taken under the disciplinary procedure (see Paragraph 11). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

10 Monitoring of use of systems

10.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, is continually monitored by **[use of automated software OR [OTHERWISE]TBA]**. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

10.2 A CCTV system monitors the exterior of the building [**DETAILS OF OTHER AREAS TBA**] 24 hours a day. This data is recorded.

10.3 We reserve the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

10.3.1 to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

10.3.2 to find lost messages or to retrieve messages lost due to computer failure;

10.3.3 to assist in the investigation of wrongful acts; or

10.3.4 to comply with any legal obligation.

11 Inappropriate use of equipment and systems

11.1 Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with our rules, policies and procedures (including this policy, the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure). See Paragraph 9, Personal use of systems.

11.2 Misuse or excessive use or abuse of our telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with under our Disciplinary Procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

11.2.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

11.2.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

11.2.3 a false and defamatory statement about any person or organisation;

11.2.4 material which is discriminatory, offensive, derogatory or may cause embarrassment to others;

11.2.5 confidential information about us or any of our staff or clients (which you do not have authority to access);

11.2.6 any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or

11.2.7 material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

11.3 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary such information may be handed to the police in connection with a criminal investigation.

12 Monitoring and review of this policy

12.1 The Head of the IT Department in conjunction with the **[COMMITTEE] AND/OR board TBA]** and **[RELEVANT BODY, FOR EXAMPLE UNION OR WORKS COUNCIL TBA]** shall be responsible for reviewing this policy [**FREQUENCY TBA**] to ensure that it meets legal requirements and reflects best practice.

12.2 The Head of the IT Department **OR [POSITION TBA]** has responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.]

12.3 Staff are invited to comment on this policy and suggest ways in which it might be improved..