



Information, Communications & Technology Services (ICTS)

Regulations for the Use of College Computing Facilities

Revised June 2006

Contents

1. [Introduction](#)
2. [Scope](#)
3. [Code of Conduct](#)
4. [Usernames and Passwords](#)
5. [Acceptable Use](#)
6. [Unacceptable Use](#)
7. [Monitoring of Use](#)
8. [Breach of the Regulations.](#)

Appendices

- Appendix 1 [JANET Acceptable Use Policy](#)
Appendix 2 [JANET Computers and the Law](#)

1. Introduction

It is not St Martin's intention by publishing these regulations to impose restrictions that are contrary to the established culture of openness, trust and integrity. The College is committed to protecting its employees, students, partners and the College from illegal or damaging actions by individuals, either knowingly or unknowingly. College data, information systems and services are to be used for academic and business purposes in serving the interests of the College, and of our clients and customers in the course of normal operations. Effective security is a team effort and it is the responsibility of every computer user to read and understand these guidelines and to conduct their activities accordingly.

This document provides important information, codes of conduct and regulations relating to the use of all St Martin's College computer, electronic information and communication facilities. These regulations are partly imposed by external providers of networks and software, such as the JANET Acceptable Use Policy (Appendix 1). There are many pieces of legislation that are relevant to these regulations. These are too numerous to list in full and are subject to regular change. The key items of legislation relevant to the use

of computer systems are summarised in Appendix 2. This is a JISC document entitled Computers and the Law.

2. Scope

St Martin's College computing facilities are available to all staff, authorised partners and registered students of the College. These regulations encompass all College data, information systems, computing and communications system and services that are owned or leased by the College. These regulations also apply to privately owned devices when they are used to access these facilities.

3. Code of Conduct

The following code of conduct must be adhered to by all members of the College community at all times:

- 3.1 All users of College computing facilities must not, through any act or omission, engage in any conduct which prevents, obstructs, disrupts or otherwise has an adverse effect upon staff carrying out their duties.
- 3.2 Students and staff are expected to use College computing facilities and equipment carefully and with consideration to others.
- 3.3 Smoking and eating in College computing facilities is prohibited. Drinking is permitted but only from sports style bottles.
- 3.4 With the exception of guide dogs, no animals are allowed in College computing facilities.
- 3.5 Children of staff and students are not permitted in College computing facilities. In particular and exceptional circumstances permission may be given by the Principal or delegated representative to waive this ruling. This regulation does not apply to children or young adults legitimately on site as in the case of organized visits.
- 3.6 Visitors and other non College members are not permitted to access College computing facilities except those persons legitimately on site as in the case of organised conferences and visits where prior arrangements for access has been made.

4. Usernames and Passwords

Computer users must not disclose their username or password, and must take all reasonable precautions to ensure that their user account details remain confidential. Any user who discloses their user account details to another individual will be held responsible for any improper actions committed under that username. If you believe that someone else knows your password you must change it. Your local Help Desk can assist you in doing this.

The use of another individual's username and password is not permitted. In exceptional circumstances permission to access another persons account may

be granted by a senior Human Resources manager.

5. Acceptable Use

College computing facilities may be used for:

- Teaching, learning and assessment
- Research
- Educational development
- Administration and management of College business
- Development work and communication associated with the above
- Consultancy work contracted to the College

Reasonable and occasional use of computer facilities for personal correspondence (email and internet access) is at present regarded as acceptable so long as this does not compromise the work and mission of the College or detract from a person's effectiveness in their work. In addition, the facilities must not be used for the purpose of any individual's non-college business activities.

Prior permission from the Principal or delegated representative, as appropriate, must be obtained in writing if use could possibly fall outside of the terms defined above.

6. Unacceptable Use

St Martin's College computer facilities, and any external network accessed from these facilities, may not be used for any of the following:

6.1 The access, creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

6.2 The access, creation or transmission of material which is designed or likely to cause annoyance, offence, inconvenience or needless anxiety.

6.3 The creation or transmission of defamatory material.

6.4 The transmission of material such that this infringes the copyright of another person.

6.5 The transmission of unsolicited commercial or advertising material.

6.6 The use of unlicensed software,

6.7 Deliberate unauthorized access or modification to facilities or services or other misuse of network resources.

6.8 Deliberate activities with any of the following characteristics:

- Wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems;
- Corrupting or destroying other users' data;
- Violating the privacy of other users;

- Disrupting the work of other users;
 - Using College computing facilities, or other external networks, in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - Continuing to use an item of networking software or hardware after being requested that use cease because it is causing disruption to the correct functioning of College computing facilities or other external network;
 - Other misuse of College computing facilities or networked resources, such as the introduction of computer "viruses".
- Where College computing facilities are being used to access another institution's network, any abuse of the acceptable use policy of that institution will be regarded as unacceptable use of College computing facilities.

7. Monitoring of Use

The College reserves the right to monitor the activities of all users of College computing facilities to ascertain whether a breach of the regulations has occurred.

All Internet and Email transmissions to and from College computing facilities are recorded and may be scrutinized to ascertain whether a breach of the regulations has occurred.

Specifically monitoring is undertaken in the areas of:

- Maintaining effective operation of networked communication systems through preventing transmission of computer viruses and reducing SPAM email;
- Preventing unauthorized use of facilities by monitoring access to web-sites and restricting access where unacceptable use is discovered ;
- Monitoring network service standards

8. Breach of the Regulations

8.1 The College has the right to withdraw a computer user's access to College computing facilities in circumstances where that person has breached the regulations.

8.2 The College may temporarily suspend a computer user's access to College computing facilities where the College reasonably believes that person may have breached the regulations, pending an investigation into the suspected breaches.

8.3 A breach of the regulations may also constitute a criminal offence, for example under one or more of the legislative documents listed in the appendices. In the event that the College suspects that a person may have committed a criminal offence, the police or other appropriate enforcement authority may be contacted to investigate whether a criminal offence has been committed.

8.4 A breach of the regulations may also breach professional codes of conduct and may lead to matters being reported to a professional body; in the case of students the breach of regulations could lead to discontinuation on a

professional course.

8.5 In addition to the above sanctions, a suspected breach of the regulations, such as the access, creation or transmission of any offensive, obscene or indecent images, data or other material, is likely to be regarded as gross or serious misconduct and will therefore be investigated and decided upon in accordance with the College's Disciplinary Procedures. In the case of staff this will be dealt with initially by the Head of Department.

8.6 A computer user who is in breach of the regulations will indemnify and extricate the College against all costs incurred by and losses caused to the College, or others, by reason of such breach, including but not limited to: repair costs; any claim for damages; legal costs; fines or other financial penalties.

Appendices

Appendix 1 JANET Acceptable Use Policy

<http://www.ja.net/services/publications/policy/aup.html>

Appendix 2 UKERNA fact sheet – Computers & the Law

<http://www.ja.net/services/publications/factsheets/005-computers-and-the-law-0606.pdf>