COMPUTING FACILITIES USE POLICY

1. INTRODUCTION:

1.1. Warwick Students' Union recognises the significant benefits of effective use of electronic forms of communication and working.

1.2. It is committed to complying with legislation and good practice in order to meet its obligations as an employer and an ethical membership organisation.

1.3. Specifically, this policy sets out the aims, procedures and responsibilities that fulfill this requirement. It clarifies what is **deemed acceptable usage of computers and what is unacceptable**. The Students' Union has policies and a user guide in relation to associated areas and these should be referred to where applicable.

1.4. The policy has been drafted in with reference to University of Warwick Regulations and the JANET Acceptable Use policy as the Internet Services Provider.

2. DEFINITIONS: (For the Purposes of the Computing Facilities Use Policy)

WSU	Warwick Students' Union
Computing Facilities	(a) any computer or device capable of storing data in electronic form owned, operated or loaned by the WSU whether connected to the WSU or partner's information network/s or not; *and/or* (b) any computer or device capable of storing data in electronic form owned or operated by someone other than the WSU when connecting to the WSU's information network or used to gain access to the WSU's information network; *and/or* (c) any computer or device capable of storing data in electronic form owned or operated by someone other than the University when used for WSU Activity; *and/or* (d) any software or information provided or created for WSU Activity; *and/or* (e) any Cloud or hosted or similar internet delivered service through which WSU information is stored and/or services are provided for the University to enable Users to undertake WSU Activity, including without limitation, email, MSL database, social media accounts.
WSU Activity	Any activity conducted either in the course of employment or as part of or related to other WSU activity that is not purely personal.
Users	All people authorised to use the Computing Facilities for any purpose, including but not limited to employees, volunteers including clubs' and societies' officers, contractors, students on work experience, WSU members, committee members, Trustees and SSLC representatives.
Confidential Data	Any data that is subject to the Data Protection Act 1998 (namely data relating to living individuals), any data that is commercially sensitive (sales, financial information, contract information)and/or any data that is indicated as such by the person sending or creating it

Harassment	The creation, transmission, accessing or sending of material which is likely to or intends to cause offence. In respect of computer use, this means any unwanted conduct/ communication based on gender, age, race, ethnic origin, sexual orientation, disability, religious belief, political belief, appearance affecting the dignity of men and women at work.
Defamation	Published, unsubstantiated, critical statements relating to an individual, organisation or group of individuals.
Bullying	The creation, transmission, accessing or sending of material which is likely to or intends to intimidate. In respect of computer use, this means persistent, offensive, abusive, intimidating, malicious or insulting communication, which makes the recipient feel upset, threatened, humiliated or vulnerable, which undermines their self-confidence and which may cause them to suffer stress.

3. POLICY STATEMENT

3.1. The policy aims to:

- Provide guidance to ensure technology is used effectively and efficiently to further the activities of WSU and to maintain the confidentiality, integrity and/or availability of electronic information
- Strike a balance between an employee's legitimate right to respect for their private life and the employer's legitimate need to run its operations and protect Warwick Students' Union (WSU) from the consequences of misuse or illegal activity
- Set out the responsibilities of all those who use the WSU network and its IT facilities
- Provide consistency about acceptable and unacceptable usage
- Ensure that procedures fit with other organisational policies
- Inform users about the legal risks to which they may inadvertently expose themselves and the organisation should the confidentiality, integrity and/or availability of electronic information be compromised
- Facilitate productive relationships between the organisation and all those who use its IT facilities
- Clarify who to contact with any queries
- Prevent damage to systems or breaches of confidentiality, integrity and/or availability of electronic information
- Minimise time spent on non-work related activity

3.2. All users are required to abide by this policy and should report any suspected, attempted or actual breaches of this policy to the Chief Executive or in their absence the Finance Director as soon as reasonably practicable. *Any attempted or actual breach of this policy and other relevant policies or procedures may lead to the suspension or withdrawal of a user's authorisation and may lead to disciplinary action or dismissal*. Refer to the Users' Guide for information on examples of conduct constituting misconduct or gross misconduct.

3.3. This policy forms part of the terms and conditions of appointment of employees and a copy should be signed on appointment and whenever required by the management of the WSU. Breaches by employees may be dealt with under the disciplinary procedures contained in those terms and conditions.

3.4. Students (members) found in breach of this policy may be subject to disciplinary action under the Students' Union Disciplinary procedure.

3.5. WSU may also take any appropriate legal or other action against any user.

4. LEGAL FRAMEWORK

4.1. This policy also provides the means to articulate and assure the WSU's compliance with relevant legislation or other requirements.

4.2. WSU will abide by all UK legislation and relevant legislation of the European Community and any other agreed legal jurisdiction related to the holding and processing of information. In the case of apparent contradiction between the WSU's policies and regulations and legislation, the latter takes precedence. Further information on the key legislation can be found in the User Guide.

5. RESPONSIBILITIES:

The Trustees:

The Trustees are responsible for:

- Ensuring that WSU has adequate policies in place, that these are reviewed regularly and that the policies comply with the law.
- Ensuring that any breaches of the law which put WSU at risk are reported, investigated and mitigating actions are taken in accordance with relevant procedures.
- ensuring that any significant incidents are reported to the Charity Commission where this is required

Finance Director:

The Finance Director is responsible for:

- reviewing this policy in light of technological changes
- ensuring that policy relating to recording of breaches of this policy is implemented

IT Team:

The IT Team are responsible for:

- Monitoring computer systems in accordance with the Data Protection Act, the Regulation of Investigatory Powers Act 2000 and other relevant legislation as it develops.
- Advising on technological changes that impact on this policy
- Providing practical guidance for users on the application of this policy
- Implementing policies and procedures relating to computer use.

Human Resources Director:

The Human Resources Manager is responsible for:

- communicating this policy to all new members of staff and for communicating changes to this policy to all members of staff
- responding to breaches of policy that may result in disciplinary action
- providing training for employees regarding this policy
- ensuring that this policy is integrated into Students' Union Student Training Programme and all Officer Training

Line Managers:

Line managers are responsible for:

- Communicating this policy to all members of staff and ensuring queries are directed to the appropriate person

- Dealing with breaches of the policy as and when they arise in accordance with the relevant procedures (e.g. Training, Discipline, Harassment, Bullying)
- Encouraging a non-discriminatory, non-intimidating working environment

Employees:

Employees including but not limited to agency or contract workers and volunteers are responsible for:

- Following this policy and associated WSU computer use procedures
- Reporting any breaches of computer use that they become aware of

The President:

The President is responsible for:

- Ensuring all WSU members are aware of and understand this policy and any associated procedures relating to computing facilities use

WSU Members:

Members are responsible for:

- Following this policy and associated organisational computer use procedures
- Reporting any breaches of computer use that they become aware of

6. SECURITY

6.1. The WSU network and Computing Facilities are intended for business use. Occasional and reasonable personal use is permitted provided that it does not interfere with the performance of your duties and/or WSU systems. See Section 7.1.1

6.2. Users will manage the risks associated with the use of a personal or shared computer or device for WSU Confidential Data. Refer to the Users' Guide for further guidance.

6.3. Where users of the Computing Facilities are issued with a WSU username and/or password, they will not share passwords with another person, or use any WSU password as login credentials for any non-WSU account. Refer to the Users' Guide for further guidance.

6.4. Users must not use existing passwords from personal accounts (e.g. email accounts, banking, and online sites) for WSU systems to limit personal and WSU risk exposure.

6.5. Unauthorised access into or from the company's networks is forbidden, as is any attempt to gain access.

6.6. All Users using their own devices to access Computing Facilities must use a password or PIN to secure access to Confidential Data kept or accessed on such devices to ensure that this data is protected in the event of loss or theft.

6.7. Copying or any attempt to copy any of the software installed on a workstation constitutes a breach of this policy and may result in disciplinary action.

6.8. All non-Union owned equipment brought into the building to be connected permanently to the network must be checked by the IT department prior to use. If non-Union owned equipment is brought into the building, it is the responsibility of the IT Department to ensure legality of the software and contents held on it. If suspicion should arise then a report will be made to the relevant authorities. This will be:

- Federation Against Copyright Theft (FAST) for suspected illegal software.
- Human Resources Manager if material is in breach of any of the WSU's personnel policies or procedures.

6.9. WSU recognises that there may be occasions where personal devices are used to access WSU computing facilities and information. The risk of the use of such device lies with individual user and must be in accordance with WSU policies and user guides.

6.10. Users of Computing Facilities should log off or access devices locked when not in use.

6.11. Users with access to Confidential Data must take all reasonable steps to prevent against loss or inappropriate disclosure.

6.12. All computers or devices including personal devices will be equipped with a suitable antivirus program.

6.13. Users will not knowingly introduce any viruses or other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware onto the Computing FacilitiesAll suspected or actual cases of viruses or other harmful programs or similar computer code as described above should be reported to the IT Team via helpdesk@warwicksu.com and copied to the Finance Director.

6.14. Remote access to WSU computing facilities and information is permitted only via the Virtual Private Network (provided by the University of Warwick). In exceptional circumstances, IP restricted remote desktop connections may be permitted only with prior authorisation from Chief Executive. Further information on remote access is provided in the user guide.

6.15. For support purposes, IT staff may require to connect remotely to your workstation. Before a connection is attempted, the user should be notified. If the user is absent and the need to access urgent, authorisation should be obtained from the Chief Executive or, in his/absence, the Financed Director.

6.16. Unauthorised copying, transmitting, downloading or using files in breach of the Data Protection Act, copyright or intellectual property is forbidden including use of removable media such as memory sticks and CDs. Prior authorisation to perform such activities should be sought from the relevant Head of Department.

7. PERSONAL USE OF COMPUTING FACILITIES OWNED OR OPERATED BY WSU

Incidental, reasonable personal use of all Computing Facilities owned or operated by the WSU is permitted provided the use is minimal, does not interfere with WSU commitments, does not put the WSU in disrepute and does not contravene our Internet Service Provider's policy on acceptable use.

8. INAPPROPRIATE USE OF COMPUTING FACILITIES

8.1 Users shall not use the Computing Facilities or any e-mail or Internet services used on the Computing Facilities:

8.1.1 To view, create, transmit or store material which could be considered inappropriate, offensive, obscene, indecent, abusive, harassing, bullying, derogatory or defamatory and/or adversely affect the reputation of the WSU or any partner organisation. Where such a question might arise, prior permission should be sought in writing from the Chief Executive; *or*

8.1.2 For any unlawful or fraudulent act, including infringing the copyright of another person; *or*

8.1.3 To send unsolicited or unauthorised advertising, promotional or any other similar material, save where that material is embedded within, or is otherwise part of, a service to which the user or the WSU has chosen to subscribe.

9. INTERNET USE (including website creation)

9.1 The use of the internet is granted to each user on the basis of the need to use it in the course of their employment. The WSU reserves the right to withdraw access on either a permanent or temporary basis if there is reasonable belief that the provision is being exploited.

9.2 WSU also reserves the right to limit time allowed for Internet browsing.

9.3 WSU reserves the right to block certain websites.

9.4 Websites for clubs and societies should normally be hosted on a WSU or University web server. Clubs and societies are representatives of WSU and its policies. All content held on a website should reflect this.

9.5 Should it be considered essential for a club or society to establish a registered web address outside of WSU or University of Warwick domains, it should be set to redirect to a website held on the University or WSU webserver.

10. MONITORING STATEMENT

10.1 Monitoring is undertaken with due regard to the Regulation of Investigatory Powers Act 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

10.2 The organisation reserves the right to undertake covert monitoring but this will only ever be undertaken in the following circumstances when there is a specific and justifiable suspicion:

10.2.1 The prevention or detection of crime;

10.2.2 The protection of systems from viruses and threats such as hacking; *and/or*

10.2.3 The investigation or detection of unauthorised use of the systems which would lead to severe system damage or unlawful acts.

10.3 The Chief Executive (or acting Chief Executive) must give authorisation to any covert monitoring before it commences.

10.4 Due regard will be paid to the Data Protection Act and other relevant UK and European Community legislation.

10.5 Changes to monitoring arrangements on a temporary basis can only be authorised by the Chief Executive.

10.6 Changes to monitoring arrangements that form part of this policy must be approved by the Board of Trustees.

11. MONITORING OF EMAIL AND INTERNET USE

11.1 Message tracking records of email traffic are kept for 28 days. They are monitored automatically. Emails from customers to individual WSU email accounts will be deemed to be intended for the business rather than the individual.

11.2 Personal emails will not be accessed, although they are recorded, unless there is a legitimate business need to do so, for example as part of a formal disciplinary investigation or where there

is suspicion that criminal activity is taking place.

11.3 If during the course of monitoring, data that would be categorised as Sensitive Personal Data under the Data Protection Act is accessed, and would be used for purposes other than those communicated to the data subject, authorisation must be sought from the Chief Executive to use the data for the new purpose.

11.4 The WSU does not normally monitor the content of emails. However, it does reserve the right to do so in certain circumstances under the terms of the Regulation of Investigatory Powers Act 2000.

11.5 Where unplanned absence occurs and emails need to be accessed for a relevant business purpose, authorisation will be sought from the Chief Executive or in their absence the Finance Director to access the relevant emails. Emails that are clearly personal or irrelevant will not be accessed.

11.6 IT staff will not view other users' email messages other than to the extent that this may occur as a consequence of their normal work. E.g. dealing with a delivery failure. Only the Chief Executive or in their absence, the Finance Director can give permission for them to view an email in order to investigate an incident.

11.7 Logs of websites visited from each computer terminal are kept for a period of 3 months.

11.8 Downloads from websites are logged and where found to be in breach of the law or the Students' Union Equal Opportunities policy, Harassment or Bullying policies, further investigation will take place.

11.9 Where individuals using the Students' Union server download material in contravention of Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988, the police will be notified.

12. PRINTING

12.1 Printing facilities are proved for the sole purpose of WSU related work. Limited personal printing is only allowed for specific and urgent needs. This must be authorised by the user's Head of Department and a charge will be made.

12.2 Printing will be monitored and charged back to the user's department. An audit trail is available for most network printers and can be used to question an employee's usage. Where a member of a staff is found to have been using the printers for personal use, they will be charged at the external customer rate for the cost of the printing.

12.3 Printing Logs for a department may be requested by the Head of Department where they suspect abuse of the printing facilities are taking place.