St Mary's University Twickenham London

Information Technology

IT Policy

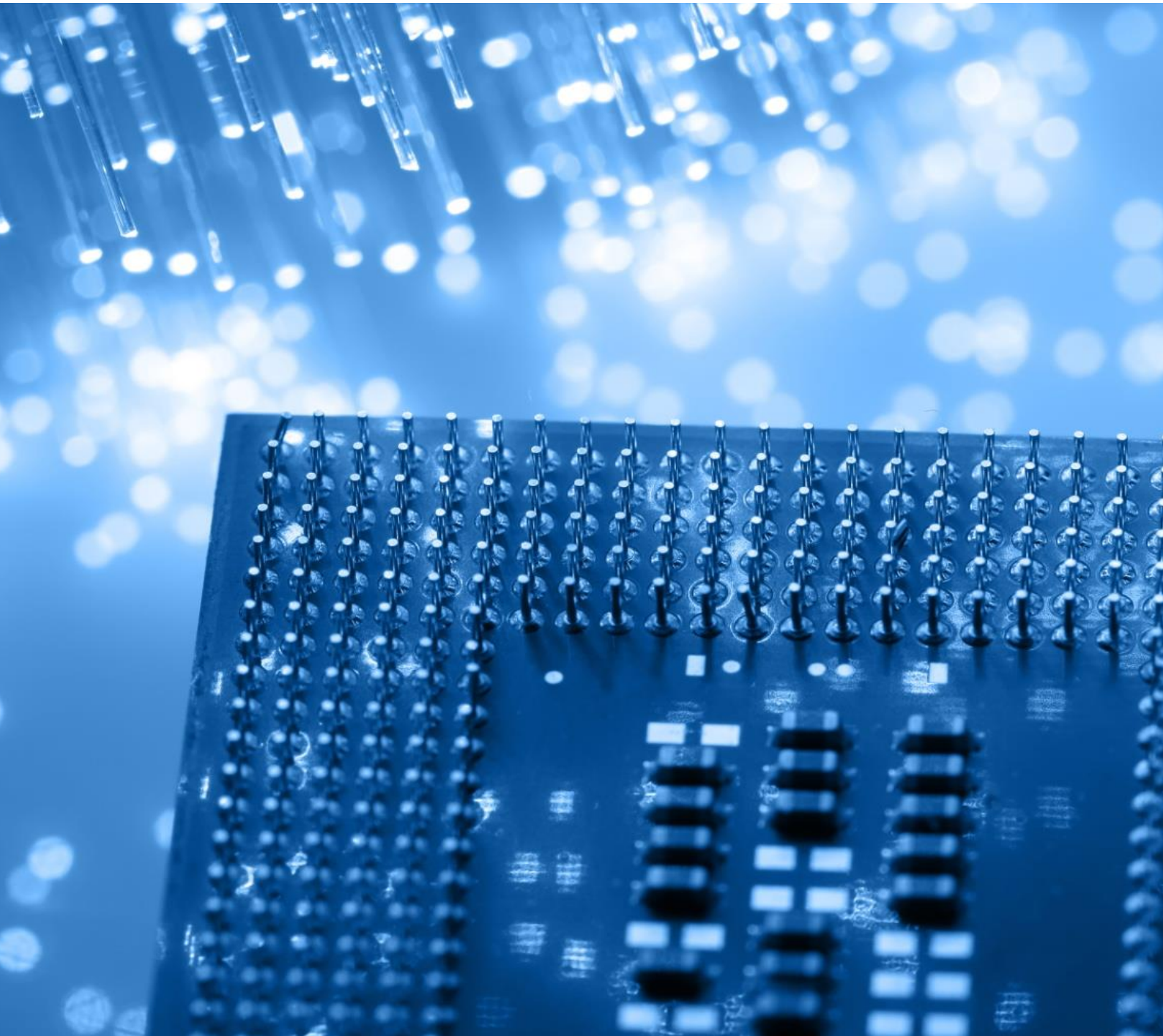

Table of Contents

Introduction

This policy applies to and governs the use of all IT systems used at St Mary's University for electronic communication and content creation, ensuring the security and resiliency of a high availability network whilst maintaining an accessible space for staff, students and visitors to communicate and collaborate online.

St Mary's University is fully committed to all legislation applying to the use of Information Technology in the United Kingdom. Where possible the University is also committed to implementing best practice in this area in order to protect the interests of the organisation, its students and staff.

The IT network and the computer systems connected to it are critical to administrative, teaching, study, employment, communication and research activities of the University, therefore to take full advantage of the benefits offered by these systems, users must familiarise themselves with this policy and adhere to the regulations set out in it. Included within this policy are guidelines on data backup, threat prevention, password compliance, usage restrictions, intellectual property, privacy rights and measures required to keep services running securely and efficiently. Additionally, powers available to enforcement of policy breach are clearly construed to facilitate fair and justifiable consequences of misuse.

Furthermore, the policy outlines the responsibilities of System Administrators and their roles in maintaining, improving and troubleshooting issues with systems connected to the University network.

Opening Statement

St Mary's University is fully committed to all legislation applying to the use of Information Technology in the United Kingdom. Where possible the University is also committed to implementing best practice in this area in order to protect the interests of the organisation, its students and staff.

Scope of the Policy

St Mary's communication facilities are provided by St Mary's University for students and staff (together = **Users**) to discuss issues of academic, administrative and general interest, to facilitate administration of the University and to communicate and collaborate online.

The IT network and the computer systems connected to it are critical to administrative, teaching, study, employment, communication and research activities of the St Mary's University (together, "**Academic Purposes**"). The ability of students and staff to use computers (whether owned by the University or devices belonging to students and staff), email and access the internet using ever-evolving technologies and platforms provides new opportunities for the University as it facilitates the gathering of information and communication with fellow employees, customers, contractors and other contacts. At the same time, this opens up new risks and liabilities. It is therefore essential that users read this policy and make themselves aware of the potential issues involved in using computers, email and the internet, when used for communication purposes or generating, storing, publishing and sharing content.

This policy applies to and governs the use of all systems used by St Mary's for electronic communication and content creation and storage including (but not limited to):

- The Internet;
- email,
- eResources,
- Turnitin,
- SimmsCAPital,
- Simmspace,
- Staffnet,
- Forums and other social media hosted by St Mary's
- IT networks,
- telephone communications
- general computing & communication systems, data, computer software, software licenses and supporting technologies

Owned by, and used within St Mary's University (together – "**St Mary's Systems"**), whether accessed directly from University property or otherwise.

This policy also covers usage of third party systems such as Facebook where they are used for purposes in relation to St Mary's University.

Policy Objectives

The objectives of this policy are to ensure that:

- relevant laws are adhered to at all times;
- the usage of St Mary's Systems for Academic Purposes and limited personal use can take place in a safe and stable environment that is adequately protected against misuse or abuse by appropriate security measures;
- any communication and user generated content is legal and appropriate and does not seek to intentionally cause offense to others;
- communication facilities are not used to bring the University into disrepute;
- users' information is preserved in privacy and integrity wherever possible subject to provisions laid out in the Privacy and Confidentiality section of this policy;

- all system administrators and users understand their own responsibilities for protecting the IT network;
- an effective high availability network operates at all times, and that rapid tracking down and resolution of any network problems by the Information Technology department (IT) is facilitated;
- interruptions to the service and unnecessary calls on support staff are minimised.

The policy will be reviewed on an annual basis.

General principles

St Mary's Systems are provided to students and staff for lawful work-related purposes. Computers and email accounts are the property of the University. Limited personal use of internet and email in breaks and before and after normal working hours is permissible but is subject to usage restrictions detailed below in this Policy. In open access areas priority should always be given to Academic Purposes.

The use of St Mary's Systems is a right granted to all Academic, Administrative and support staff, and registered students or collaborative partners with registration numbers of the University. In return, all users have responsibilities relating to use of St Mary's systems. If usage regulations are breached, access may be withdrawn at any time by the Director of IT or his/her deputy ("**Designated Authority**") In addition, the University reserves the right to exclude anyone from St Mary's Systems who fails to comply with the provisions of this policy.

Access may be granted for other users at the discretion of the Director of IT or his/her deputy.

All users sign to confirm that they agree to comply with this policy when completing the application form for a computing account, and by signing a declaration the user accepts, and will abide by these, and all other applicable regulations, when using the facilities.

Access and use by users of St Mary's Systems constitutes continued acceptance of the terms and conditions set out in this policy and take effect from your first use of St Mary's Systems.

Code of Conduct

The following section outlines the guidance and responsibilities of all St Mary's system users.

Access

When you are granted access, you will be given a login to the University Network, an email account, access to a staff or student intranet server, access to the Internet and an area to store data for academic or administrative purposes.

Authorised users have access to computing facilities and network services located at St Marys and other sites. With these facilities there are direct and implied responsibilities on the part of the University and on the user which are outlined in this section.

Online Collaborative Tools and Social Networking

St Mary's Systems include email and discussion boards for asynchronous communication as well as chat for synchronous communication (together – "**Online Communication Facilities"**).

Users should observe the following code of conduct:

- Treat others with courtesy and respect. Users should not make derogatory or personal remarks about other users and their views about employees, students, competitors or any other person in any Online Communication Facilities that are viewable by other users. Any written derogatory remark may constitute libel. Users should contact IT if they receive mail which they find offensive. The original message should not be deleted.

- Email should be treated in the same way as formal written correspondence and the same standards of behaviour apply. Users must not transmit email that intentionally causes annoyance, inconvenience, or needless anxiety to other people.

- Email is a permanent form of written communication and material can be recovered even when it is deleted from your computer.

- Communications which are confidential or of a sensitive nature should not be disseminated unnecessarily.

- You may want to obtain email confirmation of receipt of important messages; however this is not always possible and may depend on the external system receiving your message. If in doubt, confirm receipt of important messages through alternative means.

- Email is a tool to send and receive messages and should not be treated as a permanent storage medium. You should regularly delete unnecessary emails to prevent over-burdening the system. Emails and attachments which you need to retain for record keeping purposes should be saved to prevent issues arising when you near your mailbox quota.

- Try not to create email congestion by sending trivial messages or unnecessarily copying emails.

  All staff and students have a quota of data which can be held in their mailbox and folders. This can easily be reached when email messages are kept in Outlook, particularly if these contain attachments.

- When using Online Communication Facilities you should not copy or forward messages unnecessarily. As an example copying personal or commercially sensitive messages to another person without the author's permission may be a breach of confidentiality.

- Reasonable private use of email, the Internet and Social networking is permitted but should not interfere with your work. The contents of personal emails must comply with the restrictions set out in these guidelines. Excessive private use of the email system during working hours may lead to disciplinary action and may in certain circumstances be treated by the University as gross misconduct.

- By sending emails on the University's system, you are consenting to the automated processing of any personal or sensitive data contained in that email.. If you do not wish the University to process such data you should communicate it by other means.

- All emails sent outside St Mary's are accompanied by the St Mary's standard notice which is available to view on StaffNet. (https://staffnet.smuc.ac.uk/services-departments/library-IT/services-for-staff/Pages/Email-Disclaimer.aspx).

- All University business conducted via email should use the official University system.

- Staff must not enter into contracts or use emails as an official method of ordering goods or services, unless permission has been granted to do so by the Director of Finance.

- Users should access University email on a regular basis.

- The sites accessed by you must comply with the restrictions set out in these guidelines. Accessing or attempting to access inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the University as gross misconduct.

- All access or attempted access to the Internet is recorded on the University Internet filtering software. These records will be inspected with due authority if misuse is suspected.

Detailed advice on how to manage your e-mail can be found on the portal at https://staffnet.smuc.ac.uk/services-departments/library-IT/services-for-staff/Pages/Email-Management.aspx

If you require further assistance please contact the Helpdesk (helpdesk@smuc.ac.uk).

Network

Users should observe the following code of conduct:

- Never deliberately interfere or attempt to interfere with the operation of the network or computer systems

- Do not operate any equipment or software designed to eavesdrop on network communications.

- You must take reasonable steps to ensure that your use of the University network or services does not cause an excessive amount of traffic on St Mary's internal network or its external network links. IT may, pending investigation, disable computers or user accounts which appear to cause unreasonable consumption of network resources

- Do not log in to more than one PC, unless the Designated Authority has granted permission

User Generated Content

User generated content must at all times comply with the rules laid down by this policy in the "Usage Restrictions" section. While the University does not exercise editorial control over any content generated by users, it reserves the right at its sole discretion to remove from its systems any content which breaches the terms of this policy.

File Storage

Users should observe the following code of conduct:

- Do not gain access or attempt to gain access to any files owned by someone else unless the owner has specifically granted access or a 3rd party data access request has been granted

- Never use equipment in contravention of the law

- Anti-virus products must be used at all times. You must not introduce malicious code including viruses, network worms, Trojan horse, logic bombs, spyware or any other form of malware

- Do not download or install software / attach hardware to the network which may compromise the security of our data, the network or other users

- St Mary's provides each user with backed up storage for academic and administrative purposes. Users should not use third party storage or synchronisation systems for the storage or dissemination of College related material without written authorisation to do so from their Head of School or Service in consultation with the Director of IT (e.g.: use of Drop Box)

Software and Software Licences

IT will not install any software on St Mary's hardware where the correct licences have not been purchased or there is an insufficient number of correct licences in place.

Software will not be installed on computers in open access or teaching labs outside of the 'computer build period' as defined in section 6a of the Software Policy (http://staffnet.smuc.ac.uk/services-departments/library-IT/Documents/Library-IT-Policies/Software.pdf).

The installation of demo or evaluation software will only be actioned where its use complies with the licence i.e. evaluation software should be used to evaluate if the product should be purchased and not used in place of a licensed copy.

Security

Viruses and Malicious Code

All computers used within the University that are owned by the University require the current version of our Anti-Virus software to be installed. If a user suspects that their computer does not have the software installed they should immediately contact the Helpesk.

If connecting a personally owned device to the University's Wi-Fi system, it is the responsibility of each individual user to ensure that they have the latest anti-virus software installed on their device.

Users must not interfere with the operation of the Anti-Virus software installed on University-owned devices, or change its configuration, unless the Designated Authority has granted permission.

Users must scan all portable media (USB sticks, memory cards, etc.) for viruses prior to use.

If you receive any suspicious electronic communication or suspect your machine is infected by malware please contact the Helpdesk for assistance.

Intrusion and Hacking

The regulations surrounding network security are laid down in the St Mary's University General IT Policy (see Network Security section p16).

Users must in no way attempt to gain access to internal or external systems to which they have not been granted access. This includes browsing the network drives without authorisation.

Users must take all reasonable precautions to prevent other persons from using their account to gain access to internal or external systems.

Backup of Data

It is the responsibility of the user to ensure that they store their files on the network drive. The University does not take responsibility for loss of data if users do not use the network drive.

The University accepts no responsibility for the loss of data due to outage, neglect, actions or inactions of members of staff, or security breaches. No claim shall be made against the University for the loss or alleged loss of data.

All files on network drives are backed up daily to disk and weekly to tape for offsite storage, if needed up to 30 days of data can be restored.

Equipment

Laptops and Portable Equipment

Laptops and portable devices owned by the University are subject to the same policies and regulations as desktop machines. These are covered in detail in the Computer and Network Administration Policy section below.

Extra care should be taken to ensure that laptops and portable equipment (e.g. pen drives) are kept securely. Members of staff are responsible for data held on items of portable equipment.

Upon leaving employment with the University, members of staff should return laptops and/or portable equipment to HR or departmental administrator.
Old, faulty or unused laptops or portable equipment should be returned by members of staff to the IS Service Desk. Alternatively, a job can be logged for it to be picked up by a member of staff.

Any equipment returned to the Service Desk shall have any data and/or software removed from it. The equipment shall be reused, recycled or disposed of depending upon its age and usability.

Use of Personal Equipment

Users may not connect personal equipment to the University data ports except in the circumstances outlined below.

Permission may be granted to connect personal equipment to the wired network at the discretion of the Network Manager, provided it meets required standards, and has been Portable Appliance Tested.

Password Policy

User ID / Password

Users should at all times comply with the following guidelines:

- Authorised users are allocated a Login (a single username and a single password, or several pairs as required), and must ensure that nobody else uses it. The user is responsible for the security and confidentiality of the username and password.
- Users must not use anyone else's username/password.
- Users must not obtain or try to obtain anyone else's password.
- Users are explicitly prohibited from divulging their passwords to third parties (except as defined in the next section). Users must not allow anyone else to use their account even with their supervision. Users may be held responsible for the actions of, and any consequences of, any other individual using their account. Users must inform IT immediately if they suspect someone else of using their user id/password.
- Passwords must never be written down, printed or stored on-line.
- Passwords should be changed at least once every 90 days.
- Passwords should by cycled with at least five other passwords before the same password is used again, i.e. when you change your password it should not be the same as any of your previous five passwords.
- Passwords must be at least six characters in length, or the maximum allowed by that system if less than six.
- Passwords must contain three of the following types of characters, uppercase alphabetical, lower case alphabetical, numerical, or symbols (See the password guide for examples).
- Passwords must not be obvious to third parties, i.e. using your name, username, or words such as 'password' are not acceptable.
- Office computers must not be left unattended when logged in unless a password protected screen-lock is used (Windows key + L).
- The use of password protected screen lock is recommended to all users. The use of password protected screen lock is mandatory for users working with data covered by the Data Protection Act 1998.
- Shared computers must not be left unattended when logged in.
- Phone voicemail should be protected by setting up an access PIN code. This should be a minimum of six digits, not easily guessed.

Password Policy Exemptions and Special Circumstances

Users and/or System Technical Support may be required to change passwords or security settings at the request of the Director of IT if there is a possible security risk.

Local administrative account passwords on PCs will only be changed on an annual basis, during rebuilds or as part of a replacement cycle, except under exceptional circumstances arising as set out above.

If a departmental or personal administrator is required to access systems such as email on behalf of a senior member of a School or Service, then the senior member of staff is permitted to grant security permissions to the administrator.

A line manager may request access to the email or files of an employee in exceptional circumstances. Requests should be made by the Head of School or Service using the Third Party Access Form available from the staff portal.

Users should not use the same PIN number for their voicemail service as their telephone extension. Please contact the IS Staff Helpline for advice on changing your PIN.

Usage Restrictions

In addition to items already outlined in the above sections on Code of Conduct such as those outlined in the Security and Software and Software Licenses sections, you are not permitted to use St Mary's Systems for:

- Activities not directly connected with Academic Purpose (excluding reasonable and limited use for personal social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation. This includes but is not limited to
    - participation in distributed file-sharing (kazza, p2p, torrents etc.) networks
    - Using University software, software licenses, telephone, Internet and email facilities for private profit.

- Creating, accessing or attempting to access, download, transmit, forward or post any material and user-generated content which might reasonably be considered to be obscene, offensive, illegal, hateful, abusive, sexist, racist, threatening or defamatory to other people or organisations.

- Anti-social behaviour, such as
    - Harassment or intimidation
    - Person to person aggression whilst using Online Communication FacilitiesWilful disregard for others
- Any unlawful activity, including but not limited to
    - encouraging or perpetrating unlawful acts, including misuse of St Mary University software licenses
    - copying and removing data files or copyright restricted programs from the University computers or networks on any removable storage media
    - creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right in contravention of Data Protection legislation or the Telecommunications Acts
    - the sending of any communication that does not correctly identify the sender or attempts to disguise the identity of the computer from which it was sent, or the authority of the sender
    - tampering with communications that are not the user's, or making any alteration to any information
    - creating, distributing or forwarding on spam communications
    - misusing, gaining or attempting to gain unauthorised access to any facility or service within or outside the University, or any part of the system accessed through St Mary's Systems, or making any attempt to disrupt or impair computer and network services, including accessing or attempting to access other user accounts
    - storing personal data derived from St Mary's Systems

- The deliberate or reckless undertaking of activities such as may result in any of the following:

- the waste of staff effort or network resources, including time on any system accessible via the University network
- distributing any virus or other malware intended to cause nuisance, loss, corruption of or disruption to any information on St Mary's Systems or accessed through them, or of any devices used to operate St Mary's Systems or any systems accessed through them, or to any user data stored thereon
- violation of the privacy of other users
- disruption of the work of other users
- deliberate or careless introduction or transmission of malware into or through the network
- disrupting the flow of communications in interactive areas in any other way
- disruption or exposure to potential risk resulting from importing unknown files or messages on to the St Mary's network

- Causing any form of damage to the University's computing and network facilities or any of the accommodation or services associated with them.

The above list is not exhaustive, but gives an indication of examples of St Mary's Systems' misuse that is not permitted by University.

Misuse of St Mary's Systems, including third party systems where it concerns the University, can be treated as misconduct and will, in certain circumstances, be treated by the University as gross misconduct. On behalf on an appropriate external authority e.g. the Police, the University reserves the right to access the content of any University email or of any content created or downloaded onto University IT systems.

Data Protection

Users are bound by the St Mary's University Data Protection policy (available on the University Staffnet portal)

Intellectual Property

Intellectual Property Rights

Unless otherwise indicated, St Mary's Systems and their contents are the property of St Mary's University (the University). English law and international trademark law protect any trademarks.

Contributions to discussion boards and synchronous chat are regarded as the intellectual property of the authors. If they are to be quoted by another person in a publication (electronic or printed) acknowledgment must be given. Work undertaken by staff in the course of employment belongs to the institution or in accordance with current intellectual property policy.

Where the contribution of any St Mary's system user to a discussion board, synchronous chat site, email, blog, (social networking) website or other online communication system incorporates material of which that user is not the author, proper acknowledgement to the author of that material shall be given in the contribution and users will be responsible if copyright or confidentiality is breached.

Copyright and Downloading

Copyright and the use of copyright materials within the United Kingdom (UK) is governed by the Copyright, Designs and Patents Act 1988 (CDPA 1988) and the subsequent legislation and licences that St Mary's subscribes to.

The University maintains St. Mary's Systems for learning, teaching and administrative purposes. Users may access those parts of the systems to which they are entitled (e.g. module contents for their programme) and may download or copy the available learning and teaching material for private study that constitutes non-commercial use. Without prior approval, copying, distributing or use of the materials contained in St Mary's Systems for any commercial purpose is not permitted. Access and use constitutes acceptance of the terms and conditions set out in this statement, and takes effect from first use.

Copyright applies to all text, pictures, video and sound including lectures, however captured or disseminated. Files containing such copyright protected material may not be downloaded, forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

Copyrighted software, including screen-savers, should only be downloaded in accordance with the terms of the software licence.

We recommend that staff and students familiarise themselves with the University's copyright guidelines, particularly when Staff are preparing material for use on St Mary's IT Systems. Staff and students of the University living and working in countries outside the UK should familiarise themselves with the copyright legislation of the country in which they are residing, as the use of copyright material in a country is governed by that country's legislation.

Monitoring

The University has the right to monitor any aspect of its telephone and computer systems that are made available to you.

The following monitoring measures are in place:

- Software installation and usage is monitored as part of the Universitys on going software audit.
- All access to computers and network resources is logged and routinely monitored by IT staff as part of the day-to-day operation of the network.
- Additionally, St Mary's University would like to draw everyone's attention to the fact that Closed Circuit Television is in operation for the protection of employees and students.

The Designated Authority may, on behalf of the University, authorise access to communications, data and logs in accordance with UK law. . A formal process requiring signed approval by the designated authority exists for internal third party access to electronic media in exceptional circumstances.
As both this document and the email disclaimer informs users of this, the University is not required to seek further permission for monitoring from any parties involved.

Privacy and Confidentiality of Information

The provisions of this policy aim to protect the privacy and confidentiality of users' information as long as it has been created for Academic Purposes AND is not stored in email format and has not been communicated over the internet.

No expectation of privacy and confidentiality should be taken with regard to emails or Internet use, whether it is for academic purposes or personal use.

Any personal data stored within the facilities we provide should not be considered private.

Users must treat as confidential any information which may become available to them through the use of St Mary's system and facilities and which is not clearly intended for unrestricted dissemination. Such information shall not be copied, modified, disseminated, or used either in whole or in part without the permission of the person or body entitled to give it.

Users are provided with storage facilities by St Mary's University. Users must not use third part storage systems or synchronisation systems for storage and transmission of College related material unless specifically authorised to do so.

Breach of Policy

Reporting Misuse or Accidental Breaches of Policy

If a user is thought to be in breach of any of the University's procedures or regulations, including this Policy, they must be reported to HR or Director of IT or their deputy who will take the appropriate action. Access to facilities may be withdrawn pending an investigation into the actual circumstances. Upon receiving such a report the Director of IT may, on behalf of the University, authorise the investigation and or monitoring of logs. The result of such an investigation may result in disciplinary proceedings.

Should a user accidentally go to, or be redirected to, a website prohibited in the General IT Policy (Usage Restrictions section p12) they should inform the Director of IT or their deputy of the incident as soon as possible.

Disciplinary Procedures

This policy is subject to, and in addition to the law. In addition, St Mary University reserves the right to take disciplinary actions against users breaching the policy.

Any user who violates this or any other related policy may be subject to:

- Denial of access to IT systems
- Suspension of his/her computing account
- Disciplinary action as described in the Staff and Student handbooks, including action taken for misconduct or gross misconduct if appropriate; or
- Civil or criminal prosecutions under UK, European, or International Law depending on the severity of the breach.

Automatic withdrawal of facilities will occur upon discovery that a student has accessed the account of another student. A five day suspension may be imposed on the student who accessed the account and an immediate ten day suspension will be imposed on the student who granted access to the account.

Network Security

The network permits high speed connections to the Internet and is at present operated with a minimum of restrictions to enable flexibility of communications between connected computers. This flexibility of operation, however, poses potential security risks. In order to safeguard the stability, integrity and security of the University IT network, steps need to be taken by IT and each department to ensure that machines under their control are properly managed to minimise the risks.

Computer and Network Administration Policy

The following general policy statement applies to all computers in the University:

- All computers, computer peripherals, telephone and mobile phone equipment, software and software licenses procured by St Mary's University and that are used at St Mary's are the property of St Mary's University and do not belong to individual members of staff or students
- Every device connected to the St Mary's University wired network must be subject to formal system administration
- Responsibility for administration and security of computers is held by the IT department.
- The staff assigned to the system administrator role must have adequate time in which to undertake the maintenance of computers under their control. SLAs are in place for staff carrying out local administration rights work
- Access to any network connected computer must be via a logon process that identifies and authenticates the user, except where read-only access is given to certain systems (e.g. the Library Catalogue), or unprivileged access is normal and appropriate safeguards are in place (e.g. Web browsers in kiosk mode, access to a contained website)
- Any networked system which will be unused for extended periods (typically several days or more) should be switched off
- Accounts which remain unused for 30 days are disabled where possible. These accounts are deleted after 90 days
- Accounts used by system administrators should be disabled immediately after departure of member of staff
- No shared accounts will be created, except where absolutely necessary, and under the condition that a list is kept of the users of the account, and that they are jointly responsible for any action taken using the account
- Accounts should not be re-used, except where absolutely necessary, and under the condition that details are kept of the users of the account and passwords are changed.
- Lists of users and their data (such as user ids) must not be available to anonymous users or, where possible, to other users and systems administrators
- Computers in open areas should be physically secured
- Computers in other areas should be accessible only by authorised persons, and security imposed as appropriate
- Only IT Network staff may run computers running server side processes including, but not limited to, file and print servers, web services, proxy services and logging facilities
- Personal equipment may not be connected to the wired University network except with specific permission from IT

In addition to the general policy above and the general Code of Conduct applicable to all St Mary's system users, the following sections suggest the responsibilities of two other distinct groups:

- IT Administrators and
- System Administrators (School /Service Administrators)

Responsibilities of IT and System Administrators

St Mary's University appoints nominated Systems Administrators (or Network Administrators) who are responsible for the secure operation of computers.

The responsibilities of System Administrators include:

- Installation and maintenance of the operating system and network connection in order to reduce the chance of unauthorised access
- Ensuring that systems security patches are kept up to date where possible and such that the service is not adversely affected
- Putting in place systems monitoring in order to detect breaches in security, and alerting Network staff in the event of any breach
- Monitoring activity and/or recording traffic on the network if appropriate, including performing periodic intrusion detection testing either internally or by third party;
- Ensuring that all software is properly licensed
- Putting in place adequate backup procedures
- Installing adequate virus protection software
- Ensuring that adequate security (such as dial back) is utilized when connecting modems to allow remote management/troubleshooting
- Maintaining logging processes, and in particular ensuring that a record of logins on the computer is be maintained for one year
- Ensuring that all network shares are secure
- Ensuing that passwords are changed regularly and restricting the usage of the super-user passwords
- Disconnecting a system, individual workstation or software if necessary to protect or maintain service
- Ensuring that relevant group policies are applied
- Administering system user accounts (e.g. on SharePoint)

System Administrators should use the following guidelines in their work:

- Administrators operate within the guidelines of the *Charter for System and Network Administrators* by JANET

- Users, including systems administrators, should normally login with user ids without unnecessary ("super user" or "administrative") privileges. Privileged accounts should be used only for systems administrative work and monitoring. Super user and system administrator passwords should be passed to IT or School/Dept. Computer staff for use in emergency

- When undertaking systems work demanding privileged user status, administrators should login in under their own account before assuming privileged status (to maintain audit information)

- Administrators must not amend any audit or system information which may be used as part of an audit trail in cases of security breach

Responsibilities of IT Administrators

In addition to the above (for systems maintained by IT), IT will also

- Liaise with external organizations (such as JANET and UCISA) in the development and maintenance of the network
- Inform network staff of security information, hacking attempts, tools etc. via an email list;
- Provide information and good practice guidelines
- Assist LTS to correct a security breach, especially where the integrity of the network may be at risk, or it is affecting systems elsewhere
- If necessary to protect and maintain service, disconnect a system, individual workstation, software, School network or building from the wider University network
- Maintain central checking of malicious code, including of email passing through central mail systems
- Maintain site licences of virus protection software
- Co-ordinate the development and maintenance of the security policy
- Provide assistance in developing router-filtering rules if required

Termination of Accounts

Computing accounts will be terminated by IT when users cease to be a member of staff, or a registered student, or when the term/purpose for which they have been granted access ends.
Staff Accounts are usually disabled within 1 day and deleted after 90 days. A staff account may be kept open longer in exceptional circumstances. Student accounts are usually disabled after 30 days and deleted after 90 days.

The Designated Authority reserves the right to terminate or suspend computing accounts in exceptional circumstances.

Legal

Indemnity

Users are personally responsible for the content of their emails and their contributions to discussion boards, synchronous chat or similar forums and shall indemnify the University against any liability incurred by the University (including liability in defamation and for breach of copyright), which arises out of any such communication or contribution.

Each user of St Mary's Systems undertakes that he or she will not hold the University liable for any material contributed to a discussion board or synchronous chat by another person, which is defamatory of that St Mary's user.

Applicable Laws

English law governs these terms and conditions, and English courts have exclusive jurisdiction in relation to them.

Nothing in these terms of use is intended to, nor shall it, confer any benefit on a third party under the Contracts (Rights of Third Parties) Act 1999.

If St Mary's University does not enforce any right against you, this does not constitute the waiver of such a right.

If a court having competent jurisdiction finds one of these terms illegal or unenforceable, the invalidity of that provision will not affect the validity, legality, and enforceability of the remaining terms.

As a guide many of the UK and European laws that apply to computer use can be found in Appendix I of this document. A definition of terms can be found in Appendix II.

Disclaimer

The University makes no warranty that information contained on any St Mary's System is complete, accurate or up-to-date. The University takes no responsibility for the results of reliance on any such information.

The University reserves the right to vary, change, alter, amend, add to or remove any material on any St Mary's system.

The University makes no warranty that use of any St Mary's system will be uninterrupted, virus-free or error-free; or that use will not affect other software or operating systems used to access St Mary's Systems.

The University makes no warranty that use of St Mary's Systems will not infringe the rights of any other person or organisation; or that it is of reasonable quality or fit for any particular purpose, even if the University received notice of an intention to use any St Mary's system for that purpose.

The University accepts no liability for any loss or damage suffered by other parties as a direct or indirect result of using St Mary's Systems, including loss of profit, loss of opportunity, loss of business, and consequential loss, to the extent permitted in law.

You may contribute to any communication facilities (e.g. discussion boards or chat sessions) that you have access to on St Mary's Systems, provided you follow the code of conduct (set out above) for the use of St Mary's Systems; your use is only authorised on that basis. Persons submitting material to St Mary's Systems are solely responsible for the material and any claims relating to its content, whether made against the University or otherwise. The opinions of such persons are those of the individuals making them, and not of the University. The University accepts no responsibility for such opinions or any claims resulting from them. Internal disciplinary procedures for staff and students will be used in appropriate circumstances.

St Mary's University reserves the right at its sole discretion to remove any user generated content about which it receives notification that it considers objectionable. The University may remove such content whether or not the objection is sustainable. In addition, the University reserves the right to review, edit or delete any comments posted by users deemed defamatory, unlawful, threatening or otherwise objectionable. It accepts no responsibility or liability for any material communicated by third parties, to the extent permitted in law.

Contributions must not consist of, or contain, illegal or offensive material; any material which is considered by the University to be illegal or offensive may be removed from the system. For this purpose the expressions illegal and offensive include (without limitation) material the publication of which is defamatory or would infringe copyright of a third party or which contravenes Data Protection legislation or the Telecommunications Act and material which constitutes incitement to racial hatred or which is offensive or obscene.

Where a Site contains links to other websites that are owned and operated by third parties the University makes no representations with regard to the content of those websites and accepts no responsibility in respect of the accuracy, legality, decency or relevancy of those websites and we reserve the right in our absolute discretion to terminate the link to any third party websites.

Other Related Policies

Users of St Mary's University's computing facilities are also bound by the following policies:

- St Mary's University General IT Policy
- St Mary's University Data Protection Policy
- JANET Security Policy
- IT Asset Management Procedure
- Institutional Access to Staff and Student IT Accounts and Equipment
- Regulations of any third party systems to which users connect using St Mary's Systems

Appendix I

The following UK and European Laws apply to the use of computers, this list in not exhaustive and are subject to change:

- Copyright, Designs and Patent Act 1988
- Copyright (Computer Programs) Regulations 1992
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Trade Marks Act 1994
- Regulation of Investigatory Powers Act 2000
- Waste of Electronic & Electric Equipment Directive
- Uniform Computer Information Transaction Act
- Obscene Publications Act 1959 & 1964
- Protection of Children Act 1978
- Consumer Protection (Distance Selling) Regulations 2000
- Defamation Act 1996
- The Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of information act 2000
- Regulation of Investigatory Powers Act 2000

IT Department, 28th March 2014