1. Scope

Users

These regulations apply to **anyone** using the SIRM's IT facilities. This means more than students and employees of the College and its related companies. It could include, for example:

- contributors to the SIRM's web presence, and people accessing the institution's online services from off campus.
- external partners, contractor and agents based on site and using the SIRM's network, or offsite and accessing the institution's systems.
- visitors using the institution's Wi-Fi services.

IT facilities

The term IT facilities include:

- IT hardware that the SIRM provides, such as computers, laptops, tablets, smart phones and printers
- software that the institution provides, such as operating systems, office application software, web browsers etc. It also includes software that the institution has arranged for you to have access to, for example special deals for students on commercial application packages
- data that the SIRM provides, or arranges access to. This might include online journals, data sets or citation databases
- access to the network provided or arranged by the institution. This would cover, for example, Wi-Fi, connectivity to the internet from College computers
- online services arranged by the institution such as Office 365 and Pearson online resources
- IT credentials, such as the use of your institutional login, or any other token (email address, smartcard, dongle) issued by the SIRM to identify yourself when using IT facilities.

2. Governance

It is helpful to remember that using IT has consequences in the physical world.

Your use of IT is governed by IT-specific laws and regulations (such as the College's IT Acceptable Use Policy), but it is also subject to general laws and regulations such as SIRM's general policies.

3. Domestic law

Your behaviour is subject to the laws of the land, even those that are not apparently related to IT such as the laws on fraud, theft and harassment.

There are many items of legislation that are particularly relevant to the use of IT, and to do any of the below would be unlawful:

- create or transmit, or cause the transmission, 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
- distribute or circulate a terrorist publication or other material that might be a direct or indirect encouragement or inducement to others to the commission, preparation or instigation of acts of terrorism
- create or transmit material with the intent to cause annoyance, inconvenience or needless anxiety
- create or transmit material with the intent to defraud
- create or transmit defamatory material

- create or transmit material such that this infringes the copyright of another person or organisation
- create or transmit unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe
- deliberately (and without authorisation) access networked facilities or services

Below are some of the laws that explain this:

- Prevent Duty Guidance
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Counter-Terrorism and Security Act 2015
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Data Retention and Investigatory Powers Act 2014
- Human Rights Act 1998
- Data Protection Act 2018
- Regulation of Investigatory Powers Act 2000
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Defamation Act 1996 and 2013

Further information about the legal aspects of the use of IT is provided by the Jisc, see:
https://www.jisc.ac.uk/guides?f[0]=field_project_topics%3A490

4. Foreign law

If you are using services that are hosted in a different part of the world, you may also be subject to their laws. It can be difficult to know where any particular service is hosted from, and what the applicable laws are in that locality.

In general, if you apply common sense, obey domestic laws and the regulations of the service you are using, you are unlikely to go astray.

5. Authority

Authority to use SIRM's IT facilities is granted by a variety of means:

- the issue of a username and password or other IT credentials
- the explicit granting of access rights to a specific system or resource
- the provision of a facility in an obviously open access setting

Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act.

6. Use of the Internet

All internet activity is monitored by SIRM for security and personal safety purposes, and it is possible to identify individual usage.

By accessing the internet from SIRM network, students agree to the terms and conditions of SIRM Acceptable Use Policy as follows:
SIRM provides internet access to assist students in their studies. This policy cannot define every specific coursework related use of the internet. Examples of acceptable use include research for assignments and assessments, using online learning materials, or participating in forums or online groups appropriate to the course.

- Students are asked not to abuse this privilege. Any abuse may result in the withdrawal of Internet access and in the event of a serious breach will lead to disciplinary procedures,
- Some areas of the internet contain information, in textual or graphic form, which could cause offence to other people or may be illegal to download or view. Students are prohibited from knowingly accessing, viewing or downloading such material.
- Students must not bring SIRM into disrepute through use of online, 'social networking' activities.
- Examples include uploading images or videos which show antisocial behaviour or illegal activities; making derogatory statements about SIRM, its staff or other students; or revealing confidential information about SIRM, its staff or other students. This list is not exhaustive.
- Students must not use images of SIRM sites or staff, or SIRM logos, without prior permission from a manager at SIRM.
- Students are not permitted to download and/or install software.
- SIRM reserves the right to withdraw internet access for any student found or believed to be:
  - in possession of material which is sexist, racist, abusive, defamatory or obscene
  - in possession of material promoting discriminatory actions or illegal behaviour
  - in possession of any material which is in breach of copyright legislation
  - using SIRM network to obtain such material
  - using SIRM network to distribute such material
  - using SIRM network to bring SIRM into disrepute
  - downloading or installing software
  - frequently using services that are unrelated to their course, causing SIRM staff to be concerned about the effect of this activity on achievement with SIRM work
  - playing online games other than those created for learning purposes
  - using online chat services unless specifically authorised by your tutor
  - using SIRM network in any way that is disrespectful or potentially harmful to other students, SIRM staff, or the hardware and software provided by SIRM.

7. PREVENT

The college has a statutory duty, under the Counter Terrorism and Security Act2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. The filtering and monitoring of online systems to restrict access to harmful content forms part of this duty.

Members of the College community must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Systems are in place to detect this type of activity and are reported to the Safeguarding team.

Social networking is blocked in the College so the risk of radicalisation via these networks is reduced. Users who attempt to bypass college security will be subject to college disciplinary procedures.

8. Personal safety when using the Internet

There is evidence that some websites, including those used for academic purposes, are accessed by users who wish to exploit young people. You are advised to exercise care when communicating through the internet with people you do not know personally.

The following guidelines should be followed:

- Never arrange a meeting alone with someone you have made contact with on the internet
- Never disclose any personal information through the internet to unknown persons or organisations
- Be aware that any unknown persons you are communicating with through the internet may not bewho you think they are and photographs they display may not be their own

Saving and backing up your work

It is students' responsibility to save the work and one of the most important things students must learn from the start is how to do this. It is essential that students save work on own memory stick or other data storage device.

Use of Data Storage Devices (This includes CDs, DVDs, USBs and other data storage devices)

The purpose of this section is to outline the acceptable use of data storage devices on SIRM computers. USB memory devices are also known as 'memory sticks' and 'pen drives'. It is important that students read this section carefully so they understand how to safely use devices that they save their work on.

9. Conditions of Use

- Students are responsible for the information and data held on their USB memory devices.
- Students can only use data storage devices on SIRM network for their work
- Students can only use their own data storage device if it does do not require a mains electricity supply
- Powered data storage devices can only be used if they are SIRM property and are supplied through the SIRM's IT Services.
- Students are personally responsible for the correct use of your data storage device. SIRM will not accept responsibility for any data loss or damage to devices caused by incorrect connection, ejection or shutting down of computers.
- Data storage devices must not interfere with the set up of any SIRM computer hardware or software. Students are therefore not permitted to use data storage devices containing computer games, viruses, public domain software (free software), shareware, illegal copies of any kind, pornography or other

offensive materials

- To ensure that students' storage devices are virus free students should only use these on equipment with up to date anti-virus software. If students are unsure about this, they should scan the device using SIRM's virus protection software before use.
- Sensitive data or data generated and owned by SIRM, members of staff or other students, must not be copied or removed from the network without consent.

10. Intellectual Property Rights – Copyright

Copyright laws allow owners of copyrights to take legal action where materials are used without permission. Copyright laws may apply to materials published on the internet (such as text, audio, videos, movies, music or graphics), even if there is no direct statement on a website about copyright.

Users of SIRM network and IT facilities must follow the copyright laws.

Students must not:

- use illegal copies of a licensed computer program
- download, copy, store or transmit copyrighted materials without permission
- access any systems that they are not authorised to access

11. Health and Safety

This section of the policy gives guidance for protecting your health and safety while using college computers.

It is students' responsibility to:

- take regular breaks from the computer screen
- adjust chairs to support the lower back
- maintain an upright position above waist level
- tilt the keyboard using the 'props' at the back
- type with the wrists straight and with the hands in line with your arms
- place the mouse at a comfortable distance from the edge of the table to avoid stretching the arms
- adjust the screen so that eyes are at the same level as the top of the screen
- position the screen appropriately to avoid glare and adjust the brightness of the screen to the lighting conditions in the room
- leave enough room under the desk for free movement of legs
- change sitting positions from time to time
- Drinks or food are not allowed near computer terminals.
- Bags or other items must not be placed where they are in the way of anyone walking past or using another computer.
- Students must use own personal headsets on computers

12. Security and Privacy

To ensure security of the systems and the privacy of users, students must not

- access the network with someone else's details
- give own access details to someone else
- access the network through other unauthorised means

Students are advised to save the work on a regular basis, while using the system.

13. Printing

SIRM is committed to reducing the environmental impact of its activities, including the use of paper for printing. All students are asked to support this aim. Please use printing facilities for course work only, and only print out documents when essential.

14. IT Resources

Failure to comply with this policy may result in suspension of access to the network and/or disciplinary action. If students witness actions or behaviour by other students that is in breach of this policy, or notice any equipment that has been damaged or does not work, please bring it to the attention of your tutor, a manager or a member of SIRM staff.

15. Criminal Conduct

A number of activities related to the use of the internet or email are covered by law, SIRM policy and are otherwise unacceptable. Any of these activities will be regarded by SIRM as misconduct and any student involved will be subject to disciplinary action.

These activities include:

- fraud
- software theft
- terrorist activities
- on-line stalking
- grooming, internet luring, soliciting
- defamation
- retention of offensive screensavers
- retention of other people's personal details/information
- drug-related activities, or any other illegal activity

In addition, Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on SIRM to have, in the due regard to the requirement to prevent people from being drawn into terrorism.

In order to enforce this policy and ensure that IT facilities are not being misused, SIRM will randomly monitor internet usage by students.

We reserve the right to check internet usage, including pages visited and searches made as reasonably necessary in the interests of SIRM, including for the following purposes (this list is not exhaustive):

- to monitor whether the use of the internet is legitimate and in accordance with this policy
- to assist in the investigation of alleged wrongdoing
- to comply with any legal obligation

SIRM currently employs filtering to limit access to websites that contain inappropriate, offensive or illegal content. Attempted visits to these sites will be monitored by SIRM's IT Department.

16. Monitoring

Institutional monitoring

The SIRM monitors and logs the use of its IT facilities for the purposes of:

- detecting, investigating or preventing misuse of the facilities or breaches of the College's regulations
- monitoring the effective function of the facilities
- investigation of alleged misconduct

The SIRM will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

Unauthorised monitoring

You must not attempt to monitor the use of the IT without the explicit permission of the Director of Innovation and Technology Solutions. This would include:

- monitoring of network traffic
- network and/or device discovery
- Wi-Fi traffic capture
- installation of key-logging or screen-grabbing software that may affect users other than yourself
- attempting to access system logs or servers or network equipment

Where IT is itself the subject of study or research, special arrangements must be made, and you should contact your course leader / research supervisor for more information.

17. Concern about use

The internet reflects the diversity of the world. Some of the materials you may access through College IT facilities you may consider to be illegal, upsetting, or morally or ethically offensive. Accepting the rights to academic freedom and to free speech, if you are concerned about the safety and wellbeing of yourself or others, linked to use of the internet, you may contact the IT.

18. Use of Artificial Intelligence (AI)

At SIRM, we recognise the usage of modern technology and that of generative AI, is an important asset that is taking precedence. If used correctly, this new advancement can assist in a number of ways, including communication, problem solving, creative thinking, etc. In addition, it can help with enhancing the learning experience and skills development, as well as improving student performance.

The use of generative AI, however, needs to be done with care, especially when submitting an assessment. To this end, it is expected that the assessment will be wholly that of the student and any external assistance received clearly marked and referenced within the submission. Failure to do so is viewed as a serious shortcoming and action will be taken in line with the SIRM Academic Malpractice Policy.