USE OF COMMUNICATION TECHNOLOGY AND SOCIAL MEDIA POLICY

1. INTENT

The purpose of this Policy is to:

- set down the minimum standards expected by Sydney Uni Sport & Fitness (**SUSF**) for the use of its Information Communication Technology (**ICT**) resources and in relation to social media and online behaviour;
- provide notice of the workplace surveillance undertaken by SUSF, and outline the circumstances and manner in which SUSF conducts surveillance; and
- ensure that all users will be lawful, efficient, economical and ethical in their use of SUSF's ICT Resources.

2. SCOPE

This Policy applies to all users of SUSF's ICT Resources, including all employees, contractors, subcontractors, employees of contractors and subcontractors, work experience students and volunteers who perform work for SUSF; any employees of labour hire companies who have been assigned to work for SUSF; and club officials and club members (**Users**).

In addition, Users must abide by this Policy when they use social media or go online (whether using SUSF's ICT Resources or not):

(a) on behalf of SUSF or in their capacity as an SUSF employee, contractor, subcontractor, employee of a contractor or subcontractor, labour hire worker, work experience student, volunteer, club official or club member; or

(b) in a personal capacity but in any manner which may directly or indirectly impact on SUSF or an SUSF Stakeholder.

'SUSF Stakeholders' include but are not limited to: SUSF directors, SUSF managers, the SUSF Board, SUSF staff members (including employees, contractors, subcontractors, employees of contractors and subcontractors, work experience students and labour hire workers), SUSF clubs, SUSF club officials, members and volunteers, SUSF sponsors, SUSF members, staff and students of the University of Sydney, SUSF business partners, SUSF clients, SUSF competitors or sporting teams, match officials and referees.

3. POLICY

ICT Resources

For the purposes of this policy, ICT Resources include but are not limited to: mail, telephones, mobile phones, voicemail, SMS, facsimile machines, email, the intranet, software, computers, networks, servers, internet connections, hardware, equipment, printers, or other technology products or services that SUSF owns, leases or uses under licence or by agreement and any off campus computers and associated peripherals and equipment provided for the purpose of SUSF work or associated activities, or any connection to the SUSF network.

Use of SUSF's ICT Resources is restricted to legitimate SUSF purposes only. Limited minor and incidental personal use may be allowed, but it is a privilege and must not interfere with the operation of ICT Resources, burden SUSF with incremental costs, interfere with SUSF's activities, interfere with the User's employment or

other obligations to SUSF, and is subject to compliance with SUSF policies (including SUSF's Staff Code of Conduct and Workplace Conduct Policy).

Users should be aware that personal use of SUSF's ICT Resources may result in SUSF holding personal information about the User and/or others which may then be accessed and used by SUSF to ensure compliance with this, and other policies.

The use of SUSF ICT Resources through non-SUSF (including personally owned) equipment or systems is also subject to this policy.

ICT Use

To assist Users to understand the implications of the above requirements, the following examples of prohibited and permitted use are provided. These examples are indicative only.

1. SUSF will not tolerate its ICT Resources being used in a manner that is harassing, discriminatory, victimising, vilifying, abusive, rude, insulting, threatening, obscene or otherwise inappropriate.

It is unlawful to use any ICT Resource to harass, menace, defame, libel, vilify, victimise or discriminate any other person within or beyond SUSF. It is important to understand that in matters of harassment it is the **reasonable perception of the recipient** and not the intention of the sender that is significant. Refer to the SUSF Workplace Conduct Policy for more information.

Users may be individually liable if they discriminate against, harass, bully, victimise or vilify colleagues or any member of the public, or if they assist or encourage others who engage in such conduct. Users who adversely affect the reputation of another person may also be exposed to a claim of defamation by that aggrieved person.

1. Users must not use SUSF's ICT Resources to collect, use or disclose personal information in ways that breach SUSF's Privacy Policy.
2. Users must not use ICT Resources to access, store or transmit pornographic material of any sort.
3. The use of ICT Resources for gambling purposes is forbidden.
4. SUSF forbids the use of its ICT Resources in a manner that constitutes an infringement of copyright or other intellectual property rights.
5. ICT Resources must not be used in a manner that causes or could potentially cause embarrassment or loss of reputation to SUSF.
6. Users must not use ICT Resources in inappropriate ways, which are likely to corrupt, damage or destroy data, software or hardware, either belonging to the SUSF or to anyone else, whether inside or outside the network. This does not apply to specially authorised SUSF IT staff who may be required to secure, remove or delete data and software, and dispose of obsolete or redundant ICT Resources as part of their ICT Resource management duties.
7. Users are not permitted to use ICT Resources for unauthorised commercial activities, private gain or for financial gain to a third party.
8. Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to, any ICT Resource, unless they are authorised and competent to do so.
9. ICT Resources must not be used to distribute unsolicited advertising material from organisations having no connection with SUSF or involvement in its activities.
10. Users of SUSF issued accounts must identify themselves and not use a false identity.
11. SUSF email lists generated for formal SUSF communications must not be used for anything other than SUSF business.

12. Files may only be attached to email messages if the sender believes they are free from viruses and has taken steps to ensure that they do not contain viruses or other destructive code.
13. Users must not attempt to gain unauthorised access to any computer service. Users are responsible for maintaining the security of their accounts and their passwords.
14. Users must not facilitate or permit the use of SUSF's ICT Resources by persons not authorised by SUSF.
15. SUSF prohibits use of ICT Resources for purposes which include (but is not limited to) the following:
    - Violation or infringement of the rights of any other person, including their rights with respect to privacy;
    - Content that is defamatory or potentially defamatory, false and misleading, abusive, obscene, violent, pornographic, profane, sexually-explicit, sexually-oriented, threatening, racially-offensive or otherwise biased, discriminatory, illegal or any other inappropriate material;
    - Content that has instructions on the manufacture and/or use of illegal and/or dangerous products, substances or materials or any other illegal or subversive activity;
    - Violation of any SUSF policy, including prohibitions against harassment, discrimination, bullying, vilification or victimisation of any kind;
    - Forwarding of confidential messages to people to whom transmission was never authorised by SUSF, including persons within SUSF and persons/organisations outside SUSF;
    - Downloading large files that increase the load on the network and degrade the service for other staff;
    - Attempts to obtain unauthorised access to electronic communication systems, attempts to breach any security measures on any such system, attempts to intercept any electronic transmissions without proper authorisation, or unauthorised use of a password/mailbox, including constructing electronic communication so that the communication appears to be from another person/organisation/entity;
    - Broadcasting unsolicited personal views on any matter;
    - Failure to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus;
    - Propagations of chain e-mails or forwarding messages to groups or lists without the consent of the recipient;
    - Unauthorised external access of the electronic communication system;
    - Interference with the ability of others to conduct business; and
    - Actions which contradict or potentially contradict the ethos or core values of SUSF.

ICT Equipment

Users are required to take due care when using ICT Resources (including all equipment) and take reasonable steps to ensure that no damage is caused.

A User is required to refrain from using ICT Resources if they have reason to believe it is dangerous to themselves or others.

A User is required to report any damage to ICT Resources to their Senior Manager.

Monitoring and surveillance

Use of ICT Resources is not considered private. Users of ICT Resources should be aware that they do not have the same rights as they would if they were using personally owned equipment through commercial service providers.

SUSF undertakes the following types of surveillance:

1. Camera surveillance, which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place;
2. Computer surveillance, which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of ICT resources (including the sending and receipt of emails and the accessing of internet websites); and
3. Tracking surveillance, which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as global positioning system tracking devices).

This surveillance is undertaken on a continuous and ongoing basis at at all properties, buildings or other areas owned, controlled or leased by SUSF as well as any other grounds or locations at which Users will perform duties for SUSF (regardless of whether work is actually being performed at the time). Surveillance is also undertaken at other places where Users perform work for SUSF, or use SUSF's ICT resources or services.
SUSF collects, creates and stores records and information (including logs, images, backups and archives) using the following methods:

1. Telephone monitoring – SUSF monitors the input and output of fixed line and mobile phone devices provided by SUSF for use by Users.
2. Camera monitoring – SUSF had fixed security cameras throughout all of its premises, both inside and outside of buildings and other facilities.
3. Computer monitoring – SUSF monitors SUSF email accounts, emails sent or received using an SUSF email account or server, internet usage (including browsing history, content downloads and uploads, video and audio file access, and any data input or output using ICT resources), and access (including log-ons) to, and activity on, ICT resources.
4. Tracking monitoring – SUSF provides Users with equipment and devices that have functionality to monitor and record their geographical location or movement, such as mobile phones, laptops, tablets, access cards into SUSF premises, SUSF-owned vehicles with global positioning systems installed, fuel cards, and wired and wireless data point connections installed in SUSF buildings.

SUSF records and stores information, and creates records and reports, in relation to the above surveillance. SUSF may, from time to time, conduct surveillance of individual Users, and access, use and disclose information or records to monitor individual Users.

All Users should be aware that SUSF has the right and ability to audit, monitor, examine and access the content or use of any part of its ICT Resources (including any backups) if SUSF considers it necessary to do so. This includes the ability to access the content of electronic communications and files sent, received and stored using SUSF's ICT Resources.

SUSF also reserves the right to look at and copy any information, data or files (including non-SUSF material) created, sent or received by Users using, or while connected to, SUSF's ICT Resources where it considers it necessary to do so. SUSF may use or disclose information and records from surveillance it has undertaken for a range of purposes including:

1. Legitimate purposes related to the employment of employees or engagement of other Users;
2. Legitimate business activities or functions of SUSF, including internal inquiries and investigations of alleged unlawful activities or activities that are alleged to be in breach of any SUSF policies, procedures or rules, or that otherwise constitute a potential breach of a User's duties to SUSF;
3. Use or disclosure in any civil or criminal legal proceedings, to any law enforcement officials or agencies, or as required or authorised by law; and
4. Where SUSF considers it reasonably necessary to avert an imminent threat of serious violence to a person, or damage to property (including disruption to SUSF's business, systems or operations).

SUSF is also able to prevent delivery of emails sent to or received by a User, or prevent access to an Internet website by a User where SUSF considers it necessary to do so. If SUSF prevents delivery of an email, the User will be notified as soon as practicable.

Security, Confidentiality and Privacy

Matters of a confidential nature should only be conveyed or stored in an electronic format when adequate security measures have been taken.

While SUSF's communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the protection of confidentiality of any information. Messages conveyed by email and through the internet are capable of being intercepted, traced or recorded by others. Although such practices may be illegal, Users should not have an expectation of privacy and must take care with confidential information.

For further information about the personal information collected, used and disclosed by SUSF, refer to the SUSF Privacy Policy.

Communications on SUSF business in any format or media are official records. This includes email sent and received by staff members on any SUSF related matter. Care should be taken before deleting any electronic communication, to ensure that it is not required to be kept as evidence of a decision, authorisation or action. Sending an email on an official SUSF matter is similar to sending a letter on SUSF letterhead. Such email transactions should be handled with the normal courtesy, discretion and formality of all other SUSF communications. Users should not write anything in an email that they would not sign off in a letter.

Use of social media

What is Social Media?

'Social media' is an umbrella term to describe any online space where Users can connect with other people and/or produce and share content. It includes but is not limited to:

- Social networking sites e.g. Facebook, Instagram, Twitter;
- Video and photo sharing websites e.g. TikTok, YouTube, Pinterest;
- Micro-blogging sites e.g. Twitter;
- Weblogs, including blogs, personal blogs or blogs hosted by traditional media publications such as smh.com.au;
- Forums and discussion boards such as Whirlpool, Reddit, Yahoo! Groups or Google Groups; and
- Online encyclopedias such as Wikipedia and any other website that allows individual users or companies to use simple publishing tools.

SUSF Social Media Channels

SUSF and the SUSF clubs have various social media channels including but not limited to Facebook, Twitter and Instagram, which are updated on a regular basis, informing community members, staff, students and athletes on the sporting achievements of SUSF athletes and teams, in addition to various other information. The content on all SUSF social media channels (other than for SUSF clubs) is determined by the SUSF Marketing &

Memberships Department, and Users may not post content on these channels on behalf of SUSF without prior approval from the SUSF Marketing & Memberships Department.

Use of Social Media Channels

It is important for all Users to be aware that all information exchanged within social media or online networks online falls within the public domain, and the line drawn between what is considered to be personal and public is not always clear. It is also important to remember that information posted on social network sites can be easily traced and is available on an ongoing basis.

Use of social media and online behaviour by Users both in a work and personal capacity may impact the reputation, operation and perception of SUSF as well as SUSF Stakeholders. It has the potential to have a negative impact upon the way in which SUSF Stakeholders and the media view our organisation. For staff members, limited minor and incidental personal use of social media may be allowed at work, provided that it is consistent with this Policy.

Prohibited Use and Guidelines

SUSF understands that the use of social media networks and online activity is growing at a phenomenal rate and that the majority of Users are involved within the social media and online community in some personal capacity. However, a User's personal use of social media or online activities may impact on SUSF or SUSF Stakeholders. This includes (but is not limited to):

- Online activity where a User's connection to SUSF is made clear (e.g. through use of an SUSF email address or by stating an affiliation or connection to SUSF); or
- Where a User has 'befriended' another SUSF User online.

Users must abide by the following when using social media or going online:

- Ensure that online comments do not bring SUSF or any SUSF Stakeholders into disrepute.
- Carefully consider how you present yourself online (particularly given that the line between personal life and work is often blurred online).
- Do not disparage or embarrass SUSF or SUSF Stakeholders when participating in social media or online networks.
- Do not imply that any personal comments are endorsed in any way by SUSF, an SUSF Club or an SUSF Stakeholder.
- Do not post photos or personal details about other SUSF Users without their permission.
- Be careful about the information that you share which relates to SUSF. In particular, do not disclose confidential information about SUSF, Club activities or SUSF Stakeholders.
- Do not participate in social media or online networks in such a way that harasses, defames, vilifies, bullies, victimises, discriminates or treats unfairly or inappropriately any SUSF Stakeholder.
- Ensure compliance with the SUSF Workplace Conduct Policy, the SUSF Staff Code of Conduct and other SUSF policies (as applicable and as amended from time to time).
- Do not impliedly or expressly speak for or post images on behalf of or related to SUSF business operations, marketing campaigns, facilities, membership, athletes or media coverage without the express prior written approval of the Marketing and Membership Department.
- Do not use the SUSF logo or trademark without the express prior written approval of the Chief Executive Officer.

- Except when communicating official SUSF information or for directly work-related purposes, do not connect online with any child you have met in the course of delivering and managing SUSF activities and programs, at SUSF-related events or who attend or have previously attended SUSF activities and programs.

Breach and reporting

Anyone who is aware of possible violations of this Policy is required to report them immediately to an appropriate person (e.g. their supervisor, the system administrator or Senior Manager). Alleged serious or repeated breaches must be reported to the HR Manager.

SUSF reserves the right to withdraw, restrict or limit any User's access to its ICT Resources if a breach of this Policy is suspected.

Clubs will be held responsible for all content posted on club websites and may be required to reimburse SUSF for any costs associated with a breach of this Policy. Club members may also have their SUSF membership terminated for breaching this Policy. Failure by any staff member to comply with this policy may result in appropriate disciplinary action (up to and including termination of employment or engagement). In addition, Users may be requested to reimburse costs (e.g. for unreasonable personal use) and any potential criminal conduct may be referred to police.

Complaints regarding breaches of this Policy will be dealt with in accordance with the Complaints Resolution Policy.

4. ABOUT THIS POLICY

All individuals subject to this Policy are required to comply with its terms. However, to the extent this Policy describes benefits or entitlements provided by SUSF; these are discretionary in nature and are not intended to be contractual or binding on SUSF.

Subject	Use of Communication Technology and Social Media Policy
Authorised by	Chief Executive Officer
Contact	Human Resources
Version	1.0
Commencement	01 November 2020
Next review	01 July 2022