HEALTH SERVICES UNION
Internet, Email, Landline Phone and Computer Use Policy

Purpose

The Health Services Union NSW/ACT/QLD (thereafter HSU) recognises the importance and usefulness of internet, email, landline and computer facilities as research, communication and tools which are provided for work use. The availability of HSU resources for personal use is to be determined at the discretion of the HSU.

This policy sets out the appropriate standards of behavior for Users. For the purposes of this Policy, a User is defined as all HSU staffs who access or use HSU internet, email, landline and computer facilities by any means.

This policy also sets out the way surveillance of Users may be conducted in accordance with the *Workplace Surveillance Act 2005* (NSW) and the *Workplace Privacy Act 2011* (ACT).

At all times when accessing or using HSU internet, email and computer facilities, Users must ensure that they comply with this policy. It is the User's responsibility to ensure that they use the HSU internet, email, and computer facilities in a lawful and professional manner.

This policy does not form part of an employee's contract of employment or any other User's contract, except to the extent, it is incorporated by specific reference.

If you are unsure about any matter covered by this policy, you should seek the assistance of the HR.

Policy

1. Application

This policy applies to all Users of the HSU's IT systems and networks.

It applies to the use of all HSU internet, email, landline and computer facilities inside and outside working hours and inside and outside the workplace. This includes landline phones, portable computers (including iPads, iPhones and similar products), and any other means of accessing the HSU email and internet facilities, for example, a personal home computer which has access to the HSU IT systems.

2. Usage Policy

2.1 Use of internet, email, landline and computers

Users are entitled to use HSU internet, email, landline and computer facilities for legitimate business purposes.

Users are permitted to use internet, email, landline and computer facilities for limited and reasonable personal use, however any such personal use must not impact upon the User's work performance or HSU resources or violate this policy or any other HSU policy.

Users must not use internet, email, landline and computer facilities for personal use if that use interferes with the efficient business operations of the HSU.

Further, HSU email accounts should not be utilised during internal HSU election periods for the purposes of electioneering that may be deemed to be promoting a particular candidate over another.

2.2 Guidelines for use of internet, email, landline, and computers

Users must comply with the following guidelines when using internet, email, landline phone and computer facilities:

- Users must use their own username/login code and/or password when accessing HSU internet, email and computer facilities or a guest password as provided by an authorised IT Services Division Officer.
- Users in possession of HSU computing equipment (including portable computers) must always ensure that it is stored or placed in areas with a minimal possibility of theft or damage.
- Users should always protect their username/login code and password information and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.
- User must maintain the security of passwords and user accounts, follow guidelines on creating strong passwords, not sharing login credentials, and promptly report any suspected security breaches.
- Users should ensure that they log off from internet and email and lock the computer or shut down the computer when leaving the computer equipment unattended for an extended period to ensure that others do not have access to their internet, email, and computer facilities.
- If a User receives an email which they suspect contains a virus, they should not open the email or attachment to the email and should immediately contact HSU IT Services Division for assistance.
- If a User receives an email the content of which (including an image, text, materials, or software) is in breach of this policy, the User should immediately delete the email and report the matter to the Secretary/his or her direct line manager. The User must not forward the email to any other person.

2.3 Prohibited Conduct

Certain behavior is considered to be inappropriate use of HSU internet, email, landline and computer facilities and is strictly prohibited.

Users must not send (or cause to be sent), upload, download, use, retrieve, or access any email or Internet material that:

2.3.1 is obscene, offensive, or inappropriate. This includes text, images, sound, or any other material, sent either in an email or in an attachment to an email, or through a link to an Internet site (URL). For example, material of a sexual nature, indecent or pornographic material.

2.3.2 causes insult, offence, intimidation, or humiliation by reason of **unlawful harassment or discrimination**. For further information on harassing and discriminatory material, please refer to the HSU Psychological Health at Work

(Anti Bullying) Policy.

2.3.3 is **defamatory or incurs liability or adversely impacts on the image** of the HSU. A defamatory message or material is a message or material that lowers the reputation of a person or group of people.

2.3.4 is otherwise **illegal, unlawful or inappropriate**.

2.3.5 adversely affects the **performance of, or causes damage to** the HSU computer system in any way.

2.3.6 gives the impression of or is **representing, giving opinions, or making statements of on behalf of** the HSU without the express authority of the HSU.

Furthermore, Users must not transmit or send HSU documents or emails (in any format) to any external parties or organisations unless expressly authorised to do so.

2.4 Users must not use internet, email, landline and/or computer facilities to:

2.4.1 **violate copyright** or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using HSU computing facilities, except as permitted by law or by contract with the owner of the copyright.

2.4.2 **breach an individual's privacy** including breaching the HSU *Confidentiality Policy*.

2.4.3 **create any legal or contractual obligations** on behalf of the HSU unless expressly authorised by the HSU.

2.4.4 **disclose any confidential information** of the HSU or any customer, client or supplier of the HSU unless expressly authorised by HSU.

2.4.5 **install software or run unknown or unapproved programs** on HSU computers. Under no circumstances should Users modify the software or hardware environments on HSU computer systems.

2.4.6 **gain unauthorised access** (hacking) into any other computer within the HSU or outside the HSU, or attempt to **deprive or disrupt** the access or use of other Users of any HSU computing or landline phone system.

2.4.7 send or cause to be sent **chain or SPAM Emails** in any format.

2.4.8 use HSU internet, email, landline or computer facilities during working hours for **personal gain**. For example, running a personal business using HSU computers.

2.4.9 **access another User's computer or Internet access or email facilities or landline telephone** (including passwords and usernames/login codes) for any reason without the express permission of the User.

2.5 Details on blocking email or internet access

The HSU reserves the right to prevent (or cause to be prevented) the delivery of an email sent to or from a User, or access to an internet website by a User, if the content of the email or the internet website is considered:

- **obscene, offensive, or inappropriate**. This includes text, images, sound, or any other material, sent either in an e-mail message or in an attachment to a message, or through a

link to an Internet website (URL). For example, material of a sexual nature, indecent or pornographic material.

- causes or may cause insult, offence, intimidation, or humiliation by reason of **unlawful harassment or discrimination**.
- is **defamatory or may incur liability or adversely impacts on the image of the HSU**. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or a group of people.
- is otherwise **illegal, unlawful or inappropriate**.
- may affect or have the potential to affect the **performance of, or cause damage to or overload** the HSU computer network, or internal or external communications in any way.
- gives the impression of or is **representing, giving opinions, or making statements of on behalf of** the HSU without the express authority of the HSU.

2.6 Monitoring of internet, email, landline phone and computer use

2.6.1 The HSU reserves the right to keep and monitor logs of internet, email, phone conversations and computer use.

3. Workplace Surveillance

In accordance with the *Workplace Surveillance Act 2005* (NSW), we advise you that whilst accessing internet, email, landline and computer facilities, employee usage and activity may be monitored. Surveillance is applied to all Users of the HSU's IT systems and networks. Monitoring of computers and work tools is generally conducted for the purpose of managing costs and ensuring system efficiency, integrity, and confidentiality.

The HSU will not engage in real-time surveillance of Internet usage; will not monitor the content of email messages sent or received by its employees unless a copy of such message is sent or forwarded to the HSU by its recipient or sender in the ordinary way; and will not disclose any of the logged, or otherwise collected, information to a third party except under compulsion of law, or as authorised by the applicable law in force (including any amendments to the relevant legislation).

3.1 Computer surveillance

3.1.1 The HSU will undertake the following computer surveillance of staff:

- The web site visited, the duration and time of the visit and size of any downloads; and
- The number, contents and time of outgoing and incoming emails and the size of any downloads.

3.1.2 Surveillance will be undertaken by HSU IT Services Division under the supervision of the HSU Secretary.

3.1.3 The Surveillance will commence from the commencement of employment and will be continuous and ongoing.

3.2 Landline phone surveillance

3.2.1 The HSU will undertake the following surveillance of landline phone use:

- The number and length of incoming and outgoing phone calls.

3.2.2 Surveillance will be undertaken by HSU IT Services Division under the supervision of the HSU Secretary.

3.2.3 The Surveillance will commence from the commencement of employment and will be continuous and ongoing.

4. Breaches

Where the internet, email, landline and computer use policy is breached the HSU may impose a penalty and/or corrective action. Penalties and corrective actions include, but are not limited to:

- Reprimand; and/or
- Counselling; and/or
- Termination of employment.

5. Misconduct

Failure to comply with the usage requirements set out in 2.1 and 2.2 or using internet, email, landline and computer facilities in a manner listed in 2.3, 2.4 and 2.5 constitutes unacceptable use, a breach of this policy and misconduct.

Responsibility for unacceptable use lies with the employee using internet, email, landline and computer facilities.

Policy Version Control

Policy Approval Date:	30 November 2023
Approved by:	Union Council under Rule 40
Approval Resolution No:	UC 75/2023
Version No:	V2
Replaced Version No & Date:	V1 27 March 2019