Document Reference #	IHRI-ADM-POL-002
Document Title	ICT Acceptable Use Policy and Procedure
Owner	IHRI Administration
Version	1
Issue Date	01/07/2023
Next Review Date	01/07/2026

Contents

INTRODUCTION

The International Health Research Institute (IHRI, the Institute, we, us, our) seeks to provide its Authorised Users with secure and timely access to Information Communication Technology (ICT) Services to facilitate learning and teaching, research and innovation, engagement, and other functions of the Institute. IHRI uses several cloud-based ecosystems, including Google Workspace for Education. Acceptable use policies for third-party software and cloud-based programmes are found in the References section.

PURPOSE

This Policy is intended to:

- provide a clear statement of responsibilities for all Authorised Users of Institute ICT Services, including what constitutes acceptable and unacceptable use;
- outline the provision, modification, and removal of access to Institute ICT Services and
- express the commitment of the Institute to maintaining secure, effective, and reliable Institute ICT Services.

DEFINITIONS

TERM OR ABBREVIATION	DEFINITION
Account	It means a username or other identifier allowing users to access the Institute ICT Services, with or without a password.
Authentication Credential	User identification and password, username and passcode, PINs or other secret means used to access Institute ICT Services.
Authorised User	A person who has been provided with an Authentication Credential by the Institute to access Institute ICT Services.
Institute ICT Services	Facilities and services provided to an authorised user, including software, communication devices, and computing infrastructure under the control of the Institute (or a third-party provider on the Institute's behalf) that provide access to information in online or electronic format.
Institute Representative	This means a person appointed by IHRI who controls the use of Institute ICT Services.
Outside User	This means a person or organisation external to the Institute.
Personal Information	Information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
Private Cloud	A private cloud is a service operated solely for a single organisation, managed internally or by a third party and hosted internally or externally.

1. Acceptable Use of Institute ICT Services - Policy

1.1

This Policy reinforces providing a fair, safe and productive computing environment for the Institute community by establishing clear responsibilities for Authorised Users that do not adversely impact the Institute's operations, assets, or reputation.

1.2

All Authorised Users must act per this Policy and all other applicable Institute policies and procedures.

1.3

Institute ICT Services span multiple legal jurisdictions. Authorised Users are responsible for being aware of the jurisdiction that applies to their location when using Institute ICT Services.

1.4

Subject to Clause 1.5, Authorised Users are permitted to use Institute ICT Services for properly authorised and supervised business, education, or research purposes, providing that the use:

- is lawful;
- is in a responsible, ethical and equitable manner;
- is consistent with the values of the Institute as outlined in the staff and student codes of conduct;
- does not create an intimidating or hostile work or study environment for others;
- does not jeopardise the provision of a fair, safe and productive computing environment and
- does not adversely impact the Institute's operations, assets, or reputation.

Authorised Users who are unsure whether a proposed use is permitted or authorised should seek written approval from their supervising head of the organisational unit (e.g. the Director).

1.5

Institute ICT Services must not be used in any manner which the Institute considers to be inappropriate; this may include, but is not limited to:

- accessing pornography;
- unauthorised monitoring of electronic communications;
- knowingly downloading, storing, distributing or viewing offensive, obscene, indecent, or menacing material. This could include, but is not limited to, defamatory material, material that could constitute racial or religious vilification, discriminatory material, material that incorporates gratuitous violence or frequent and highlighted bad language;
- stalking, blackmailing or engaging in otherwise threatening behaviour;
- any use which breaches a law, including copyright breaches, fraudulent activity, computer crimes and other computer offences;
- transmitting spam or other unsolicited communications, or
- the introduction or distribution of security threats, including viruses or other harmful malware.

1.6

Limited personal use of Institute ICT Services is acceptable, provided that use is otherwise per this Policy. Limited personal use of Institute ICT Services is a privilege.

1.7
Authorised Users must not attempt to gain unauthorised access to Institute ICT Services (and the information stored thereon) to which they have not been given access or permit others to do so.

1.8
Authorised Users must not tamper with Institute ICT Services, which may cause performance degradation, service instability, or compromise operational efficiency, security, or fair use.

2. Authorised Access and Restriction Policy

2.1
All Authorised Users are permitted to access the Institute ICT Services at a level commensurate with their position, role, delegated authority or student status.

2.2
Per the ICT Access and Account Management Procedures, access to all Institute ICT Services will be removed when the relationship between Authorised Users and the Institute ceases.

2.3
Authorised Users must not use their access to Institute ICT Services to gain inappropriate personal, academic, financial or other advantage.

2.4
Authorised Users must maintain the confidentiality of any Personal Information accessed via Institute ICT Services.

2.5
Authorised Users of Institute ICT Services cannot provide others with their Authentication Credential(s). Authorised Users must ensure that their Authentication Credentials are securely stored, as they are responsible for all activity initiated from their account or with their Authentication Credential(s).

2.6
Authorised Users must use Multi-Factor Authentication (MFA) where supported to access their Institute account and ICT Services.

3. Software Licences - Policy

3.1
Software purchased by the Institute is licensed primarily to the Institute; however, approval may be granted to Authorised Users for use at home or other locations on non-Institute-owned computers during work or study with the Institute per the ICT Acceptable Use Procedures.

3.2
Authorised Users must comply with contractual obligations and terms and conditions of use stated in the software license agreements entered by the Institute.

3.3
Authorised Users must discontinue use and uninstall the software from a non-Institute-owned computer(s) upon cessation or termination of employment or completion of study or upon notification by the Institute of its termination of the software license agreement.

4. Monitoring and Privacy Policy

4.1

The Institute reserves the right to monitor, access, log, and analyse the activities of Authorised Users and Institute ICT Services and conduct reviews and audits as necessary.

4.2

The Institute reserves the right to block or filter any use that breaches this Policy or exceeds the Institute's acceptable level of risk.

4.3

The Institute may take any action deemed necessary to remedy immediate threats to Institute ICT Services or information and communications technology security, including, without limitation, suspending an Authorised User's access, confiscation of Institute-owned electronic devices and disconnecting or disabling equipment with or without prior notice.

5 Consequences of a Breach - Policy

5.1

Breaches of this Policy may be grounds for misconduct/serious misconduct.

5.2

Without limiting section 5.1, a breach or alleged breach of this Policy may result in a referral to the police and other relevant external authorities.

5.3

Without limiting section 5.1, the Director may immediately suspend an Authorised User's account in the case of a breach or an alleged breach of this Policy.

6.0 General Usage – Procedure

6.1

Categories of Authorised Users include:

a. Any Institute student who has been allocated an Account or who has been authorised by a member of the Institute's academic staff to use an Account;
b. Any representative of another educational institution authorised to use Institute ICT Services through an arrangement between the Institute and the other educational institution;
c. An Outside User who has been provided with an Authentication Credential or
d. Any individual associated with an Outside User is authorised to use an Account allocated to the Outside User.

6.2

Authorised Users must:

a. Take responsibility for all activity initiated from any Account through which they have been granted access to Institute ICT Services;
b. Ensure that their Authentication Credential(s) are securely stored as they are responsible for all activity initiated from their Account or with their Authentication Credential(s);

c. Not allow another person to use their Account and Authentication Credential. Similarly, an Authorised User must not attempt to initiate or operate a computer session utilising another person's Account and Authentication Credential or other means. Should an Authorised User believe that the security of an Account has been compromised, they must report this to the ICT Help Desk;
d. Not circumvent the Institute's authorised connections or subvert its security measures. This includes the 'jailbreaking' of Institute devices;
e. Only access Institute ICT Services using the Accounts they have been authorised to use;
f. Observe ICT Bulletins issued by the Institute and
g. Comply with any system quotas. If an Authorised User exceeds any of their quotas, they may be personally charged for the cost of their use and temporarily prevented from using the affected Institute ICT Service.

7.0 Personal Computer Security – Procedure

7.1

Institute staff and students who use a personal computer (including smartphones) must:

a. Take responsibility for the security of personally owned computers and equipment used in conjunction with the Institute ICT Services;
b. Familiarise themselves with ICT good practice guidelines and take reasonable steps to ensure that personal computer(s) do not threaten Institute ICT Services when connected to the Institute network. This may include:
    - Regularly scanning their device for viruses and
    - Maintaining up-to-date software versions; and
c. Protect against loss or theft of Institute data by:
    - Regularly backing up data;
    - Using encryption tools to protect sensitive data;
    - Logging off or locking devices when left unattended;
    - Implementing a secure access mechanism, such as a password and
    - Avoid leaving devices unattended in public places, even if physically secured.

8.0 Software Licensing – Procedure

8.1

The Institute has entered into various software licensing agreements with software vendors. Under the terms of those agreements, Institute staff and students may be able to install any of the products covered under the agreement onto an Institute-owned machine or personal device(s).

8.2

Refer to the Software Supplier Agreements & Offers on the Institute Intranet for information on how to access software and the terms of use, which must be complied with by staff and students.

9 Data management - Procedure

9.1

All academic research supervisors and Institute Directors are responsible for ensuring that they:

- Define research data management requirements and communicate these requirements to the relevant stakeholders, as required by the Code for the Responsible Conduct of Research.

9.2

All Institute staff and students must:

- Adhere to the data management requirements as specified by their Division;
- Ensure all electronically held Institute-owned information is stored so that it is backed up regularly. This can be achieved by:
    - storing data on institute-approved systems;
    - storing data on an Institute network drive or system or
    - storing data on an Institute-cloud-based storage

REFERENCES

Smartsheet Acceptable Use Policy

Smartsheet User Agreement

Smartsheet Security Practices

Google Workspace for Education Privacy Notice