IT Conditions of Use Policy

Purpose and Scope

To outline the conditions of use for all Information Technology systems and facilities at the University.

This policy applies to all staff, students, alumni, contractors and the public.

Murdoch University IT and communications systems are provided for the purpose of teaching, learning, research, engagement and administration in support of the University's vision. This policy specifies the responsibilities of all users of the University's IT systems and communications systems.

Objectives:

- To outline the conditions of use for all Information Technology (IT) systems and facilities at the University.
- To ensure that information technology systems function in a secure, efficient and effective manner.
- To maintain the confidentiality, integrity and availability of information.

Policy

1. SECTION I – REQUIREMENTS

1.1 Any person who uses University IT systems or facilities does so subject to applicable laws, statutes and relevant University policies, including but not limited to; the *ICT Security Policy*, *Password Policy*, *Privacy Policy*, *Copyright Policy*, and the *Violence, Aggression and Bullying in the Workplace Policy*.

1.2 Use of IT systems is subject to conditions which are designed to maintain the confidentiality, integrity and availability of facilities, services, information and information systems.

1.3 Use of shared computing facilities is subject to conditions which are designed to maintain the facilities in good order and to generate academic and administrative environments that are productive, ethical, legal, secure and effective.

1.4 Murdoch has the right to monitor and examine any information on or transiting through its systems. This includes the right to monitor and examine staff internet usage and the content of emails sent and received from Murdoch email accounts.

1.5 Users must not take deliberate actions intended to reduce the confidentiality, integrity or availability of information, IT systems or facilities.

1.6 Access must be via an authorised account. Users must adhere to the University's *Password Policy* and must not disclose their password to any other person. Users must not attempt to discover another person's password or gain access to another person's account or information.

1.7 All data access requests must follow the Data Access Request Process as described in the *ICT Security Policy*, and *ICT Security Standard*.

1.8 All University information must be stored centrally. Security and management of information that is not stored centrally remain the sole responsibility of the user.

1.9 Users are responsible for maintaining the integrity and security of all University IT devices, including but not limited to tablets, smart phones, laptop computers and desktop computers. Users must maintain devices to the standard required by the *ICT Security Policy*, which may include patching operating systems, all software applications and anti-virus software.

1.10 Connections to the campus network must be made only by specialist personnel under the direction of Information Technology Services. Users must attach appropriate equipment only at existing user-connection points. All requests for additional of network connections or relocation of a connection must be directed to the IT Service Desk (see http://goto.murdoch.edu.au/ITServiceDesk).

1.11 Murdoch University permits the connection to the network of personal smartphones and tablets for legitimate study or work purposes, subject to this policy. Guidelines on connection, permitted uses and responsibilities for personal devices are provided in the *ICT Security Standard* under section 12 Mobile Computing Security.

1.12 Murdoch University has the responsibility of safeguarding any sensitive information, including the PII (Personal Identifiable Information) of an individual such as but not limited to Staff, Student, Alumni, Contractors, public that use our facilities etc. Therefore, all Murdoch users that handle PII data must ensure personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

1.13 Users must report to the IT Service Desk and IT Security any suspected incident that might reduce the confidentiality, integrity or availability of an IT system.

1.14 The University reserves the right to limit, restrict, or extend access to IT systems at the discretion of the Director Information Technology Services.

2. SECTION II – UNACCEPTABLE USE

Unacceptable use includes, but is not limited to:

2.1 Illegal activity

The University's computing and networking facilities must not be used to create, obtain or transmit information that could result in legal action against the University.

2.2 Restricted and objectionable material

The University's computing and networking facilities must not be used to create, obtain or transmit pornography, hate, realistic and explicit depiction of violence and racially insensitive material.

2.3 Malicious Software

Users must not knowingly possess, give to another person, install on any of the computing and networking facilities, or run, programs or other information which could violate University policy, license or contracts. This includes, but is not limited to, malicious software such as viruses, Trojan horses, worms, password breakers, and packet observers.

2.4 Connection of unauthorised hardware

Users must not connect to the computing and networking facilities devices defined as unauthorised under the *ICT Security Policy*.

2.5 Copying and copyrights

Any user connected to the computing or networking facilities must adhere to the Murdoch University *Copyright Policy*.

2.6 Harassment

Murdoch's computing and networking facilities must not to be used to libel, slander, bully or harass any other person. Users must adhere to the Murdoch University *Violence, Aggression and Bullying in the Workplace Policy*.

Examples of computer harassment include, but are not limited to:

- Annoying, terrifying, intimidating, threatening, or offending another person by conveying obscene material or threats of bodily harm;
- Displaying offensive material in any publicly accessible area, such as computer screens and printers;
- Contacting another person repeatedly with the intent to annoy, harass, or bother;
- Disrupting or damaging the academic, research, administrative, or related pursuits of another person; and
- Invading or threatening to invade another person's privacy.

2.7 Misuse of resources

It is not acceptable use to deliberately perform any act which will impair the operation of any part of the computing and networking facilities or deny access by legitimate users to any part of them. This includes but is not

limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.

Examples of unacceptable misuse of resources include, but are not limited to:

- Generation of large volumes of unnecessary printed output;
- Use of large amounts of disk space;
- Creation of unnecessary multiple jobs or processes;
- Creation of heavy network traffic.

2.8 Personal use

Limited use of University computing and network facilities for personal business is tolerated but must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.). The University reserves the right to proactively monitor and manage the resources related to personal use.

University computing and network facilities must not be used in connection with compensated outside work nor for the benefit of organisations not related to Murdoch University, except in connection with scholarly pursuits (such as academic publishing activities).

2.9 Commercial use

It is not acceptable to use the University's computing and networking facilities for commercial purposes.

Examples of commercial use include, but are not limited to:

- Generating commercial gain;
- Placing a third party in a position of commercial advantage;
- Non-University related communications;
- Commercial advertising or sponsorship, except where clearly in support of the mission of the University.

2.10 Game playing and gambling

University computing and network services must not to be used for extensive or competitive recreational game playing, or for gambling. Limited recreational game playing, that is not part of an authorised and assigned research or instructional activity, is tolerated (within the parameters of each College's/Office's rules).

3. SECTION III – EXCEPTION REQUESTS

Users may apply to the Director Information Technology Services for authorisation to use the University's IT systems and communication systems in ways that would otherwise be deemed unacceptable, provided it is for bona fide purposes.

Non-Compliance:

Non compliance with this policy may result in disciplinary action under relevant statutes, policies, or other legal action. This may include removal of access to University information systems, withholding of results, expulsion or in the case of employees, suspension or termination of employment.

Governance

Approval Authority	Director, Information Technology Services
Owner	Director, Information Technology Services
Legislation mandating compliance	
Category	Primarily a function of management
Related University Legislation and Policy Documents	Copyright Policy Email and Electronic Messaging Policy ICT Security Policy ICT Security Standard Password Policy Password Standard Privacy Policy Social Media Policy Workplace Bullying, Harassment and Discrimination Policy
Date effective	01/10/2022
Review date	01/10/2025

Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
Administrative amendment	27/08/2023	
Approved	01/10/2022	
Approved	12/11/2019	

Approved	26/07/2016
Approved	01/12/2015
Approved	13/10/2014
Approved	29/03/2011
Approved	14/10/2010
Approved	24/09/2010
Approved	14/06/2010

Please refer to the electronic copy in the Policy and Procedure Manager to ensure you are referring to the latest version.