Provision and Acceptable Use of IT Policy (MPF1314)

Policy Reference	Proposed Change	Rationale
1 (d)	Updated the statement: (d) provide authority for the University to, where necessary in the performance of its functions or activities, monitor usage of University computing and network facilities to: (i) assist in the detection and investigation of actual or reasonably suspected unlawful behaviour or breach of University policy; and (ii) act on allegations of misuse of those facilities.	The statement is updated to provide greater transparency in the Objectives of the policy. The policy now makes clearer the existing practice of monitoring of usage for actual or suspected unlawful behaviour or breach of University policy.
2.1 (c-e)	Updated the statements: (c) honoraries; (d) contractors, consultants and external providers; and (e) approved visitors and other approved individuals or organisations.	This update improves the clarity on who is subject to the policy
4.10	Updated the statement: **Usage monitoring and investigations** 4.10. All actions and usage of University computing and network facilities may be logged, monitored, recorded and analysed by authorised University personnel to: • substantiate an allegation of misuse of University computing and network facilities; • facilitate the investigation of an activity that may be contrary to University policy and/or compliance obligations; or • facilitate the investigation of misconduct allegations and investigations, including where the use of the University computing and network facilities is not the subject of the suspected misconduct.	This update describes more clearly the purposes of monitoring and analysing computing and network facilities.
4.11	Additional statement added: **Use of Wireless data** 4.11 The wireless network may be monitored by the University for the following purposes: • to ensure that use of the network is authorised; • for the management of the network and related University systems and services; • to investigate use or misuse of the network in connection with a breach of any law or University policy (including but not limited to misuse as described in 5.21 of this policy); • to obtain analytical data relating to the use of the network and the physical University campus, for future planning and space/infrastructure management; • to assist in the detection and investigation of any actual or suspected unlawful or antisocial behaviour or any breach of any University policy by a network user, including where no unauthorised use or misuse of the network is suspected; and • to assist in the detection, identification, and investigation of network users, including by using network data to infer the location of an individual via their connected device. In carrying out these activities, the University may collect, use, or disclose personal information associated with the network including (but not limited to): account usernames, IP addresses, MAC addresses and network activity.	These statements have been added to separate and make clear the monitoring purposes for Wireless network data.
4.12	Additional statement added: **Access to University-provided communication and collaboration services** 4.12 Electronic communications and collaboration activities that use University computing and network facilities are records of the University. Examples include emails, video conferencing applications (including chat threads and meeting recordings and transcriptions), SharePoint sites and Learning Management System collaboration applications.	This statement has been added to provide examples of communication and collaboration services captured by the policy, including emails. The list is not exhaustive and may change over time. The intent of reference to these services is to ensure they are noted as being within scope, for clarity.
4.13	Additional statement added: 4.13 While the University recognises that some incidental, reasonable and lawful personal use of email, chat and other electronic communication channels will occur, users should note that the University may collect this personal information. The University reserves the right to access electronic communications without consent in circumstances where access to and review of the content of those electronic communications considered necessary to support actions as described in 4.10.	This statement is intended to make more explicit that some personal use of IT facilities is an acknowledged norm, but given that all use may be monitored, the information utilised in personal use may also therefore be captured.
4.14	Additional statement added: **Authorisation to access information** 4.14 Access to personal information as outlined above will require authorisation from the Executive Director, Business Services and Chief Information Officer, and will be recorded.	This statement has been included to identify that an authorising environment exists for approving access
5.6 – 5.13	The term “Provider” has been updated to “Service Owner”.	The term Service Owner is better understood by both IT and non-IT stakeholder and clearly implies ownership and responsibility for a service. It also helps to reduce potential confusion about responsibilities by distinguishing internal University roles from external service providers.
5.11 (d)	Additional statement added: (d) for the purpose of meeting regulatory or compliance obligations mandated by a government authority;	This update clarifies the responsibility of the Service Owner regarding suspension or withdrawal of any service or access of any user to facilities when mandated by a government authority.

<table>
<tr><td>5.15</td><td>Updated the statement:

5.16. Any user who becomes aware that facilities are being used by any person to infringe copyright or any intellectual property rights of another person or entity, or that the effect of any use of any facilities is to infringe such rights, must notify the University copyright officer immediately.</td><td>This update ensures that the policy explicitly defines the responsibility related to copyright rights.</td></tr>
<tr><td>5.20 & 5.21</td><td>Two additional statements added:

5.20. All users should use a secure and reliable internet connection and avoid using public Wi-Fi networks unless appropriate security safeguards are implemented.

5.21. All users must always safeguard sensitive information. This includes:

(a) not discussing or displaying sensitive information in public spaces or with unauthorised people.

(b) ensuring devices that store University data are physically secure and not leaving them unattended.</td><td>These additions reinforce essential cybersecurity best practices, enhancing data protection and mitigating risks related to insecure network connections and physical security threats.</td></tr>
<tr><td>5.22 (d)</td><td>Updated the statement:

(d) the deliberate or reckless creation, transmission, storage, downloading, or display of any defamatory, pornographic, offensive or menacing images, data or other material which may incur legal liability to the University, or any data capable of being resolved into such images or material. An exception can be made in the case of the appropriate use of facilities for properly supervised University work or study purposes, for which a prior written approval must be obtained in accordance with exception clause 4.6;</td><td>This update ensures that pornography is explicitly called out in the policy as an example of misuse.</td></tr>
<tr><td>5.22 (e)</td><td>Updated the statement:

(e) use which constitutes an infringement of copyright or any intellectual property rights of another entity;</td><td>This update ensures that the policy explicitly defines the responsibility related to copyright rights.</td></tr>
<tr><td>5.22 iv.</td><td>Updated the statement:

iv. the use, distribution, or introduction of hacking tools or malicious software (e.g., viruses, worms, trojan horses) within university IT environments. These tools will be regarded as malicious, even if utilised in an approved course, unless they are confined to isolated testing networks.</td><td>This change improves clarity and precision, ensuring that the policy explicitly defines the controlled use of hacking tools within isolated environments.</td></tr>
<tr><td>5.22 (i)</td><td>Additional statement added:

(i) creating, transmitting, storing, downloading or possessing child exploitation material, for example child pornography and material that instructs on, promotes or incites child abuse.</td><td>This addition reinforces the University’s commitment to child safety in alignment with the University’s Child Safety Policy.</td></tr>
<tr><td>5.34</td><td>Updated the statement:

5.34. If the affected user is a student, the student should be referred to the Student Appeals Policy (MPF1323) and associated process, and advised of their right to present an appeal under that policy.</td><td>This update clarifies the appropriate appeals pathway for students.</td></tr>
<tr><td>6</td><td>Additional statement added to the table:

<table><tr><th>Role/Decision/Action</th><th>Responsibility</th><th>Conditions and limitations</th></tr><tr><td>Authorise access to information under section 4.14</td><td>Executive Director, Business Services and Chief Information Officer</td><td>Access must be restricted to authorised personnel and the information accessed must be the minimum required to meet the purposes of the request. This includes de-identification where possible and prompt deletion of information that is no longer required for the stated purpose.</td></tr></table></td><td>This update reflects the addition of section 4.14.</td></tr>
<tr><td>7</td><td>Added the definition for Service owner:

Service owner means an individual who has been allocated responsibility for an information system (such as an. application, device, network, cloud service, or a specific component thereof). There is only one service owner for each information system. A service owner will commonly be delegated asset custodian responsibilities by several asset owners.</td><td>The definition is aligned to the Information Security Policy and is added due to the change to sections 5.6 - 5.13 (as mentioned above).</td></tr>
</table>