Engagement Hub

INTELLECTUAL PROPERTY RIGHTS POLICY

Protection of Intellectual Property

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	14/10/2024	Gillian Woolley	Document first created
0.1	1/7/2025	Gillian Woolley	Approved at MRM 1/7/25

2 Document Contents Page

3 Intellectual Property Rights Policy

3.1 Purpose

The purpose of this policy is to protect intellectual property rights.

3.2 Scope

All employees and third-party users.

3.3 Principles

Engagement Hub will manage its IP assets efficiently, effectively to ensure the maximum benefit of these assets.

Use of proprietary products are in full compliance with legal, statutory, regulatory, and contractual requirements.

4 Management of Internal and External Intellectual Property

IP ownership and rights are clearly addressed in Engagement Hub agreements, contracts and commercial arrangements with external parties. This includes:

- Engagement Hub maintains a register of contracts and agreements with third parties that specifies the use and ownership of Engagement Hub’s IP.
- Before using proprietary IP, we check that we are using the intellectual property with permission and or in line with the licencing agreement or contract.

4.1 Engagement Hub ownership

Engagement Hub owns, controls and manages all IP which is created by Engagement Hub staff and third party contractors pursuant to the terms of their reemployment or engagement or which is crated by a person acting under the direction or control of Engagement Hub.

- HR contracts of employment where IP created as part of an employment contract belongs to Engagement Hub.
- Third party outsourcing specifies that IP created for Engagement Hub belongs to Engagement Hub.

4.2 IP Register

All IP usage is easily identifiable through the use of an IP register and appropriate storage system for documents evidencing agreements recorded in the register. The following is captured:

- Date of contract or agreement
- Location of agreement
- Nature of agreement
- Type of IP (trademark, copyright, general)

5 Using Third Party Software – Third Party Licencing

Software used by the organisation is acquired through official channels and where a purchase is required to use the software evidence of a valid license is retained.

- Software is used in line with the licencing agreement.
- A software license register is maintained.
- Software license reviews are conducted at least annually or after significant change.
- Software patching levels are maintained in line with manufacturer recommendations.
- Only software that is supported by the manufacturer is to be used.
- Software is only installed by authorised, assigned persons.

5.1.1 Software License Assets Register

All software is registered and recorded in the Software License Assets Register.

The following is captured as a minimum

- Software Name
- Software Version
- Person Responsible
- Whether the software is free or paid
- Number of licenses purchased
- Number of licenses in use
- Location of the actual license
- Where the software is deployed
- The last review dates
- The next review dates
- Who conducted the review

5.1.2 Software Risk Management

Software is assessed for the risk to the organisation to information security before acquisition and usage.

5.1.3 Cloud Service Supplier Selection

Software selected is based on its ability to meet the needs of the business.

5.1.4 Changes to Software

Changes to how we use third party proprietary Software used will follow the Change Management Policy and Change Management Process.

Changes to existing software usage are significant changes and not to be taken lightly. This would be a significant change requiring a significant project with all associated resources and risk management and project management.

6 Policy Compliance

6.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.

7 Areas of the ISO27001 Standard Addressed

Intellectual Property Rights Policy Relevant ISO27001 Controls Mapping

ISO27001:2022	ISO27002:2022	ISO27001:2013/2017	ISO27002:2013/2017
ISO27001:2022 Clause 5 Leadership ISO27001:2022 Clause 5.1 Leadership and commitment ISO27001:2022 Clause 5.2 Policy ISO27001:2022 Clause 6.2 Information security objectives and planning to achieve them ISO27001:2022 Clause 7.3 Awareness	ISO27002:2022 Clause 5 Organisational Controls ISO27002:2022 Clause 5.1 Policies for information security ISO27002:2022 Clause 5.36 Compliance with policies, rules, and standards for information security ISO27002:2022 Clause 5.4 Management Responsibilities ISO27002:2022 Clause 5.9 Inventory of Information and Other Associated Assets ISO27002:2022 Clause 5.32 Intellectual Property Rights ISO27002:2022 Clause 6 People Controls ISO27002:2022 Clause 6.3 Information security awareness, education, and training ISO27002:2022 Clause 6.4 Disciplinary process ISO27002:2022 Clause 8.8 Management of technical vulnerabilities ISO27002:2022 Clause 8.19 Installation of Software on Operational Systems	ISO27001:2013/2017 Clause 5 Leadership ISO27001:2013/2017 Clause 5.1 Leadership and commitment ISO27001:2013/2017 Clause 5.2 Policy ISO27001:2013/2017 Clause 6.2 Information security objectives and planning to achieve them ISO27001:2013/2017 Clause 7.3 Awareness	ISO27002:2013/2017 Clause 5 Information security policies ISO27002:2013/2017 Clause 5.1 Management direction for information security ISO27002:2013/2017 Clause 5.1.1 Policies for information security ISO27002:2013/2017 Clause 5.1.2 Review of the policies for information security ISO27002:2013/2017 Clause 7 Human resource security ISO27002:2013/2017 Clause 7.2.1 Management Responsibilities ISO27002:2013/2017 Clause 7.2.2 Information security awareness, education, and training ISO27002:2013/2017 Clause 7.2.3 Disciplinary process ISO27002:2013/2017 Clause 8.1.1 Inventory of Assets ISO27002:2013/2017 Clause 18.1.2 Intellectual Property Rights