

Thriveology Wellness CIC

Acceptable Use Policy.

September 2024



ACCEPTABLE USE POLICY

September 2024

INTRODUCTION

This Acceptable Use Policy establishes guidelines for the appropriate use of Thriveology's information technology resources, including computers, networks, and internet access. The goal of this policy is to ensure a safe, secure, and productive environment for all users.

This policy applies to all employees, volunteers and other individuals who have access to Thriveology's IT resources.

ACCEPTABLE USE

Users are expected to use IT resources responsibly and primarily for legitimate business purposes. Acceptable uses include, but are not limited to:

1. Business Communication: Utilising email and other communication tools for work-related communication.
2. Research: Accessing and utilizing online resources for job-related research and development.
3. Software Use: Using licensed software and tools authorised by the organisation for performing job functions.

PROHIBITED USE

The following activities are strictly prohibited:

1. **Illegal Activities:** Engaging in any illegal activities, including but not limited to copyright infringement, hacking, and distribution of pirated software.
2. **Harassment and Discrimination:** Sending or distributing messages that are abusive, harassing, or discriminatory.
3. **Inappropriate Content:** Accessing, downloading, or distributing obscene, offensive, or inappropriate materials.
4. **Personal Gain:** Using organisational resources for personal profit or commercial activities not authorised by the organisation.
5. **Unauthorised Access:** Attempting to gain unauthorised access to any system, network, or data.
6. **Malware and Viruses:** Introducing malicious software, viruses, or any other harmful elements to the network.

NETWORK SECURITY

Users must take necessary precautions to protect the integrity and security of the network, including:

1. **Password Management:** Using strong, unique passwords and changing them regularly.
2. **Device Security:** Ensuring that devices are secured with up-to-date antivirus software and firewalls.
3. **Reporting Incidents:** Promptly reporting any security incidents, unauthorised access, or suspicious activities to the managing director or data protection officer.

MONITORING AND PRIVACY

Thriveology reserves the right to monitor and log all network activity, including email and internet usage, to ensure compliance with this policy. Users should have no expectation of privacy while using organisational resources.



COMPLIANCE

Failure to adhere to this Acceptable Use Policy may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal action.

POLICY REVIEW

This policy will be reviewed annually and may be updated as necessary to reflect changes in technology, laws, or organisational practices.

ACKNOWLEDGMENT

By using Thriveology's IT resources, you acknowledge that you have read, understood, and agree to comply with this Acceptable Use Policy.

SIGN:

NAME:

DATE:

Review Date: SEPT 2025