


Integrated Management System	C10	
WRAP IT Acceptable Use Policy		
Version: 6.0	Date: March 2025	Page 1 of 3

1. Purpose

This policy establishes guidelines for the proper and secure use of WRAP's IT resources, ensuring compliance with legal, ethical, and organisational standards. Adherence to this policy protects our assets, reputation, and sensitive information.

2. Scope

This policy applies to all employees, volunteers, contractors, and third-party users with access to WRAP's IT resources, including desktops, laptops, mobile devices, networks, software, and online services.

3. Acceptable Use of IT Resources

- **General Use:** IT resources are for business purposes and must align with WRAP's values. Personal use should be limited and not interfere with work duties.
- **Email and Communication:** Email and communication tools are for business-related communication. Limited personal use is permitted if it does not affect productivity or violate other sections of this policy.
- **Internet Usage:** Internet access is provided for work purposes. Access to inappropriate content (e.g., illegal, discriminatory, or harmful) is prohibited.
- **Software and Applications:** Only approved software may be installed or used. Users are prohibited from downloading unauthorised software or apps. Primarily this should be the Microsoft 365 Suite of tools. These should be used in the first instance where possible and appropriate.
- **Shared Resources:** Resources like printers should be used responsibly, with conservation in mind.

4. Security and Data Protection

- **Passwords and Access:** Passwords must be strong and kept secure. Sharing passwords or login credentials is strictly prohibited.
- **Data Handling and Confidentiality:** Sensitive data should be stored, accessed, and transmitted securely, adhering to GDPR and internal data protection guidelines.
- **Remote Access:** Remote access to systems should follow secure practices, including the use of MFA.
- **Prohibited Activities:** Users may not attempt unauthorised access, tamper with systems, or use IT resources for illegal activities.

5. Device Security

- **Physical Security:** Devices must be secured when unattended, screens locked when not in use and lost or stolen devices reported immediately.

- **Unauthorised Devices:** Only organisation-provided devices may connect to the network. Personal devices must only connect to the "Guest" wifi networks and must not be on the same network as company resources.

6. Cloud and External Service Usage

- **Approved Cloud Services:** Only use authorised cloud services for storing or sharing work-related files.
- **Data Transfer Restrictions:** Users may not transfer data to unauthorised cloud services or personal accounts.

7. Clear Desk and Clear Screen Policy

- **Workspace Security:** Keep sensitive documents secure and ensure desks are clear of confidential information when unattended.
- **Screen Locking:** Lock screens when away from devices to prevent unauthorised access.

8. Security Awareness and Training

- **Mandatory Training:** All users must complete regular security training, including topics like phishing, password security and Data protection
- **Annual Refresher:** Users must review and reaffirm their understanding of this policy and security best practices annually.

9. Incident Response and Reporting

- **Reporting Suspicious Activity:** Report any suspicious emails, phishing attempts, or security incidents to IT Helpdesk
- **Security:** The IT team will manage security incidents, protect users, and respond to reports promptly.

10. Change Management

- **Software and Hardware Changes:** Obtain IT approval for any changes to software, hardware, or configurations.
- **Use of Approved Tools Only:** Users must only use IT-approved tools and software to maintain compliance and security.

11. Monitoring and Privacy

- **Monitoring:** IT systems and internet usage are monitored to ensure compliance with this policy.
- **Privacy:** Users should have limited expectations of privacy when using organisation-provided devices and networks.

12. Audit and Compliance Checks

- **Random Audits and compliance checks:** WRAP may conduct random audits to ensure compliance with this policy.

13. Policy Exceptions

- Requesting Exceptions: Users may request policy exceptions for specific needs, subject to IT approval and risk assessment.

14. Enforcement and Disciplinary Actions

- Disciplinary Measures: Violations of this policy may result in disciplinary actions, up to and including termination. Legal consequences may apply in certain cases.

15. Policy Review and Updates

- Annual Review: This policy will be reviewed annually and updated as necessary. Users will be informed of significant changes.

16. Acknowledgment of Policy

- User Acknowledgment: All users must acknowledge they understand and agree to comply with the Acceptable Use Policy.