PaperWorks Online Ltd. - Acceptable Use Policy (AUP)

Policy Version: 1.0
Effective Date: [Date]
Review Date: Annually, or as required
Policy Owner: IT/System Administrator
Approved By: [CEO Name]

1.0 Purpose

The purpose of this Acceptable Use Policy (AUP) is to define the acceptable and appropriate use of PaperWorks Online Ltd.'s information technology (IT) assets, including but not limited to computers, networks, software, email systems, internet access, and data. This policy aims to:

- Protect the company's IT assets from misuse, damage, or compromise.
- Ensure the reliability, security, and availability of IT resources for business operations.
- Minimize risks to company data, including customer personal data protected under GDPR.
- Comply with legal and regulatory obligations.
- Clarify employee responsibilities regarding the use of company IT assets.

2.0 Scope

This policy applies to all Authorized Users, including:

- All permanent, temporary, and contract employees of PaperWorks Online Ltd.
- Third-party contractors, vendors, and agents who are granted access to company IT assets.
- Any other individual using company-owned or managed devices, networks, or systems.

The policy covers all company IT assets, whether:

- Owned, leased, or rented by the company.
- Accessed on company premises or remotely.
- Used for business or limited personal use (where permitted).

3.0 General Principles

All Authorized Users are expected to:

- Use IT assets responsibly, ethically, and in accordance with all applicable laws and company policies.
- Prioritize business-related activities during working hours.
- Protect the confidentiality, integrity, and availability of company and customer data.
- Report any suspected security incidents, policy violations, or vulnerabilities to the IT Administrator or CEO immediately.

4.0 Acceptable Use Rules

4.1 Account and Access Management

- Users are accountable for all activities performed under their unique user account.
- Passwords must be strong and kept confidential. They must not be shared, written down in an unsecured location, or reused for non-company services.
- Users must lock their screens (Windows+L / Ctrl+Cmd+Q) when leaving their workstation unattended.
- Users must not attempt to access systems, data, or accounts they are not authorized to use.

4.2 Internet and Network Use

- Company internet access is provided primarily for business purposes.
- Limited Personal Use: Occasional, reasonable personal use is permitted (e.g., checking personal email during breaks) provided it:
    - Does not interfere with job performance.
    - Does not consume excessive bandwidth.
    - Does not violate any other part of this policy.
- Prohibited Activities include:
    - Accessing, downloading, storing, or distributing illegal, offensive, obscene, or discriminatory material.
    - Engaging in activities that could harm the network (e.g., launching attacks, port scanning).
    - Using peer-to-peer (P2P) file-sharing networks or torrents for unauthorized software/media.
    - Bypassing network security controls (e.g., using unauthorized proxies or VPNs).

4.3 Email and Communication Systems

- Company email accounts (@paperworksonline.ie) are for business communication.
- Users must exercise caution with email content and attachments, especially from unknown sources.
- Prohibited Activities include:
    - Sending spam, chain letters, or fraudulent (phishing) emails.
    - Disclosing confidential company or customer data via unencrypted email without necessity.
    - Using email for harassment, discrimination, or the distribution of offensive material.
    - Forging or misrepresenting email headers.

4.4 Software and Systems

- Only company-approved and licensed software may be installed on company devices.
- Users must not attempt to modify, disable, or circumvent system security settings or software.

- All software and operating systems must be kept updated with the latest security patches provided by the IT Administrator.

4.5 Data Handling and Protection

- Customer Data: Must be handled strictly in accordance with the company's Data Protection & Privacy Policy and GDPR requirements. It must only be accessed for legitimate business needs.
- Confidential Information: Company financial data, business plans, and internal communications must not be disclosed to unauthorized individuals.
- Storage: Sensitive data must be stored only on approved company systems (e.g., secure cloud storage, company server) and never on personal USB drives or unapproved cloud services (e.g., personal Google Drive/Dropbox).
- Disposal: Paper documents containing sensitive information must be shredded. Digital files must be permanently deleted using company-approved methods.

4.6 Company-Owned Devices

- Laptops, mobile phones, and tablets provided by the company remain company property.
- Devices must be protected from theft or loss. They must not be left unattended in public places.
- All devices must be secured with a password/PIN and encrypted where possible.
- The company reserves the right to install necessary security software and, under defined circumstances, to remotely wipe or inspect devices to protect company data.

5.0 Remote Work & Bring Your Own Device (BYOD)

- Remote Work: When working remotely, users must follow all security policies. This includes using a secure Wi-Fi network (avoid public Wi-Fi for work tasks; use a company-approved VPN if necessary) and maintaining the physical security of company devices and data.
- BYOD: The use of personal devices (phones, tablets, laptops) for company business is not permitted for accessing core business systems (e.g., admin panels, customer database) unless an explicit exception is granted by management with specific security controls in place.

6.0 Monitoring

Users acknowledge and agree that:

- To ensure network security and policy compliance, the company monitors and logs activity on all company IT assets. This includes internet browsing history, email metadata, file access logs, and system usage.
- Monitoring is conducted in accordance with Irish law and GDPR. The company respects user privacy but does not guarantee it for activities conducted on company systems.

7.0 Policy Violation & Enforcement

- Violations of this policy will be taken seriously and may result in disciplinary action, up to and including termination of employment.
- Certain violations may also lead to civil or criminal liability for the individual and the company.
- Suspected violations should be reported confidentially to the CEO or IT Administrator.

8.0 Policy Review & Acknowledgment

This policy will be reviewed annually. All Authorized Users are required to read, understand, and comply with this policy.

Employee Acknowledgment
I, [Employee Name], have read, understood, and agree to comply with the PaperWorks Online Ltd. Acceptable Use Policy. I understand that violation of this policy may result in disciplinary action.
Signature: _____
Date: _____
For Company Use:
Date Provided to Employee: _____
Acknowledgment Copy Filed in Personnel Record: [ ]