# ACCEPTABLE USE POLICY—DIGITAL TOOLS AND SYSTEMS

[Organization Name] (hereinafter referred to as "The Company"), is increasingly embracing digital tools and technologies to modernize and streamline our workplace operations. Our goal is to ensure that all employees are well-informed about the expectations and permissible uses of these digital resources.

## SCOPE

This policy applies to all users accessing The Company’s IT resources, including but not limited to employees, contractors, visitors, and external partners.

## POLICY

This policy serves multiple purposes: it outlines the guidelines for technology use in the workplace, safeguards the Company's reputation and operational processes, and provides robust protections for employees' personal data and images to prevent unauthorized or malicious use.

### **Acceptable Use**

Users may utilize the Company’s IT resources primarily for business-related purposes. Personal use is permitted as long as it does not interfere with Company operations or productivity. For example, using the Wi-Fi network to access social media during breaks is allowed.

Device Usage

* Only Company-provided or authorized devices should be used for capturing and storing any media on Company property.
* Only Company-provided or authorized devices should be used in the access and use of programs and systems required for daily operations.

Digital Media Capture

* Machinery must be in a safe state prior to capture.
* Safety devices must never be bypassed to capture the needed media.
* Only capture what is necessary to provide value to the process or for what the applicable tool is being used for.
* Any person being digitally captured must be made aware they are doing so and for what reason.
* Every effort should be made to minimize the ability for employees captured to be identifiable in any media captured where possible.
* In the event the captured media is deliberately intended to capture the individual for external use, the individual must provide written consent for their likeness to be used.

Data Protection

Any handling and storage of personal information will strictly adhere to the Personal Information Protection and Electronic Documents Act (PIPEDA). No personal information will be disclosed internationally without proper authorization in compliance with PIPEDA.

### **Unacceptable Use**

Users are strictly prohibited from engaging in activities that are illegal, harmful, or unauthorized while using the Company's IT resources. These restrictions are not only in line with Company policy but are also unlawful. Failure to comply can result in disciplinary action and legal consequences.

Illegal and Harmful Activities

* Users may not engage in illegal activities.
* Users may not access, upload, or distribute offensive, threatening, or harmful content.

Unauthorized Use

* Users may not use IT resources for unauthorized personal or commercial activities.
* External distribution of any captured media on Company property is prohibited without the authorization of Company management. (See details in the Digital Media Distribution section.)

Consent and Harassment

* Capturing staff members for any reason without their consent is not allowed.
* Using Company property in a harassing manner is prohibited.

Legal Implications

Engaging in harassment, discrimination, or cyberbullying is against both Company policy and human rights legislation. Similarly, the non-consensual distribution of intimate images is not only a violation of our Company policy but will also lead to legal repercussions.

### **Digital Media Distribution**

Only authorized members of The Company may distribute digital media captured on Company property. Failure to adhere to this will result in disciplinary action and legal consequences.

Authorized Use and Distribution

* Only authorized members of The Company may capture, use, and distribute externally any media on Company property.
* Media may be shared externally only with written consent from someone in Company management.
* Any media captured and shared externally without authorization will be requested to be removed, and further action may be taken based on the content, especially in cases involving safety, harassment, or other offences.

Data Protection and Compliance

* Any sharing of personal information through digital media must strictly adhere to PIPEDA.

Legal Implications

Any distribution of intimate images without consent is strictly prohibited. Engaging in such activities could have legal repercussions.

### **Email and Communication Activities**

The following guidelines apply:

* Unsolicited email messages or spam are not permitted.
* Harassment or any other illegal use of Company services is strictly forbidden.

### **Software and Intellectual property**

In compliance with the Copyright Act of Canada, the following guidelines apply:

* Users will only use the apps provided to them on Company-provided devices.
* All copyright and licensing agreements must be respected.
* Unauthorized downloading, installation, or use of software is not permitted, nor is attempting to override any protections enabled to disallow these installations.

### **Enforcement**

The Company takes policy adherence seriously. Non-compliance will result in disciplinary actions, ranging from verbal or written warnings to termination of employment. Engaging in illegal activities could also lead to legal repercussions.

### **Other Information**

Anything outlined in the above policy shall not supersede the applicable federal or provincial laws governing access to data or digital use.

**Updates**

This policy will be reviewed and updated as needed to address new technologies and procedures. All staff members are to be trained on this policy.