

## **Acceptable Use Policy**

### **I. Purpose**

This policy outlines the appropriate and responsible use of Sandy River Plantation's information technology (IT) systems, internet access, email, mobile devices, and data resources to ensure security, productivity, and legal compliance.

### **II. Scope**

This policy applies to all Sandy River Plantation employees, elected officials, volunteers, contractors, and third-party users who access or use municipal IT systems, such as computers, networks, software, email, and mobile devices.

### **III. Authorized Use**

Users may access Plantation IT resources for:

- Carrying out municipal duties and services
- Communicating with colleagues, residents, or vendors
- Accessing job-related systems and applications
- Reasonable incidental personal use that does not interfere with work

### **IV. Prohibited Activities**

Users shall not:

- Access or distribute obscene, harassing, or discriminatory content
- Use municipal resources for personal gain, unauthorized political activity, or lobbying
- Circumvent security protocols or share passwords
- Download, install, or use unauthorized software or applications on municipal devices without prior approval from the Board or designated IT administrator
- Store Plantation data on personal or unapproved devices
- Use personal email or messaging accounts for municipal business

### **V. Email, Internet, and Social Media**

All email and internet activity conducted on municipal systems is public and subject to Maine's Freedom of Access Act (1 M.R.S. § 402 et seq.). Users must:

- Avoid phishing, spam, and suspicious links
- Use encryption for sending confidential or protected data
- Assume all municipal email content may be subject to public disclosure
- Do not treat any email communication as private

- Not post confidential or protected Plantation information on social media

## **VI. Data Security and Confidentiality**

All users must:

- Safeguard passwords and sensitive data
- Comply with applicable state and federal data protection laws
- Report suspected breaches or password compromises immediately
- Use encryption and secure channels when accessing or transmitting protected information

## **VII. Device and Remote Access Requirements**

Any access to Plantation data via Plantation-issued laptops, phones, or remote systems must:

- Be authorized by the Board or designee
- Require secure authentication (e.g., passwords, VPN)
- Encrypt Plantation data at rest and in transit
- Comply with lockout and timeout protocols

## **VIII. Monitoring and No Expectation of Privacy**

The Plantation reserves the right to monitor all use of municipal IT systems. Users have no expectation of privacy. Emails, files, and usage logs may be audited and may be subject to public records requests.

## **IX. Violations and Enforcement**

Violations of this policy may include, but are not limited to:

- Revocation of access privileges
- Disciplinary action, up to and including termination
- Referral to legal authorities in the case of criminal misuse

## **X. Effective Date**

This policy is effective as of **8/12/2025** and shall remain in effect until amended or repealed by the governing authority. All personnel subject to this policy are expected to comply from the effective date forward.

## **XI. Review and Contact**

This policy shall be reviewed annually within 60 days of the start of the new fiscal year, or as needed to reflect changes in technology, law, or best practice.

For questions or concerns regarding this policy, please contact:

**Ethna L. Thompson**

[sandyriverPlantation@outlook.com](mailto:sandyriverPlantation@outlook.com)

### **Acknowledgment of Receipt and Agreement**

I acknowledge that I have received, read, and understood the Sandy River Plantation Acceptable Use Policy. I agree to comply with the standards, principles, and responsibilities outlined in the policy, and I understand that it is my obligation to uphold these expectations as part of my role within the municipality.

I understand that this policy is intended to promote secure, responsible, and professional use of technology resources in service to the community. I also acknowledge that failure to adhere to this policy may result in appropriate corrective action as determined by the governing body.

By signing below, I confirm that I have had the opportunity to ask questions regarding the policy and that I accept the responsibility of reviewing and adhering to its contents.

**Name (Printed):** \_\_\_\_\_

**Position/Title:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Date:** \_\_\_\_\_