Acceptable Use Policy

CHANGE HISTORY

Date	Version	Created by	Approved By	Description of change
08/10/2024	1.0	Bharath S	Ashwin Khosla	Basic document outline and submitted for review

Scope

The Acceptable Use Policy applies to the following

- All Employees of Veranda Learning
- All Contractors of Veranda Learning
- All vendors / third-party / visitors who temporarily access Veranda Learning's equipment
- All computers/laptops
- All mobile devices
- Internet and Intranet usage
- Software procured
- Leased or rented equipment

Purpose

The purpose of this policy is to outline the acceptable use of Veranda Learning information assets and computer equipment. These rules are in place to protect the employee and the company. Inappropriate use exposes the company to risks including malware attacks, compromise of network systems and services, and legal liability.

Background

The Acceptable Use Policy outlines the rules for using electronics and computer equipment for business use. The rules in this policy are written to reduce the risk of intentional or accidental exposure of confidential and business information to third parties by improper use of company equipment and network. These rules prevent illegal, harmful, discriminatory, or abusive behavior using the company networks or property.

Policy

Acceptable use policy requires that under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing company-owned resources. The use of all resources must be strictly for the Company's business purposes.

General Use and Ownership

While the Company desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems and network remains the property of the Company.

Because of the need to protect the Company's network and information assets, management cannot guarantee the confidentiality of personal information stored by employees on any computer system or device belonging to the Company.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of clear guidance or if there is any uncertainty, employees should consult their supervisor or manager.

For security and maintenance purposes, authorized individuals within the Company may monitor security cameras, equipment, systems, and network traffic.

Veranda Learning reserves the right to audit networks, systems, and their contents (e.g., email or chat) periodically to ensure compliance with this policy.

Data Protection

Employees should take all necessary steps to prevent unauthorized access to the Company's confidential information. Examples include personally identifiable information such as employees' or customers' tax data, credit card data, birth dates, home addresses, SSN or Immigration ID numbers, phone numbers, other sensitive data, corporate strategies, trade secrets, and sales data. Employees recognize that access to such data is on a need-to-know basis.

Laptop & Tablet Security

Employees are provided with a laptop or a tablet when starting at the Company. The employee must acknowledge that they are responsible for the device's physical security allocated to them. All laptops and tablets acquired for or on behalf of the Company are company property. Employees recognize that laptops and tablets are expensive and that employees should exercise common sense in keeping these devices safe and secure. In this regard, employees must

- Store any files or documents that need backup in the Company's shared file drives or other data repositories.
- Store their laptop in a secure location when not in use.

Employees are prohibited from

- Attempting to remove or circumvent antivirus, password-protected screen savers, or other security measures installed on their laptops when given to them.
- Leaving laptops unattended outside the office in any capacity.
- Knowingly leaving PII on the laptop or sending an email can result in termination.

Confidential Conversations

Employees should not have conversations about a customer's identifiable information in the open office. It is important to remember that frequently there are potentially third parties, vendors, and others in the office.

Computer use

- Employees must keep passwords secure and should never share accounts with unauthorized individuals. Authorized users are responsible for the security of their passwords and accounts.
- Employees must not use corporate passwords for non-business-related applications and websites. Employees must use the password manager provided, and all corporate passwords must be distinct and must adhere to the corporate password policy.
- Employees must not use the password manager's master password for other systems.
- All computing devices used by the employee connected to the company network shall be continually executing approved malware-scanning software with a current virus database.
- Employees must not tamper with Anti-Malware software.
- Employees must use extreme caution when opening email attachments received from unknown senders that may contain viruses and other malware. If unsure about the origin, authenticity, or security of an email, ask someone from the technical operations staff, post in the technology channel in Slack, or send an email (WITHOUT forwarding potentially offending email and attachments) to the information security team mailbox.
- Employees must not install software from any source unless specifically authorized by the IT department. Users may download business required data files from the Internet but must check them for viruses before executing them.

- Employees must not send any sensitive data such as credit card numbers, telephone calling card numbers, personal information (e.g., Social Security numbers), or passwords through the Internet.
- Employees must use Microsoft or Google's authenticator app for a multi-factor authorization solution with their company email address.
- Employees must keep antivirus software updated and functional at all times.
- Employees must set up a screensaver with a password with a timeout of 2 minutes.

Mobile Phones

- All mobile phones must be password protected with a screensaver set to a 1-minute timeout.
- No mobile device can access data classified as secret or highly sensitive.
- Personal Electronic Equipment Use
- Employees should not bring personal computers or other electronic devices to the workplace or connect them to company electronic systems (excluding Company email or messaging applications such as SLACK or TEAMs on mobile phones) unless expressly permitted via an approved request by the Company. Those personal devices include but are not limited to desktop or laptop computers, tablets, USB memory sticks, or other portable data storage devices not owned by the Company.

Printer, copier, and fax machine use

- When printing, copying, or receiving a fax containing confidential information, the involved users must not leave the machine until all copies of the sensitive information are removed.
- All paper copies of sensitive information must be disposed of by shredding or other methods approved by the IT department.
- Confidential information must not be sent outside the Company.

Unacceptable use

- The following activities are, in general, prohibited. The list below is not comprehensive but attempts to provide examples of activities that fall into the category of unacceptable use. Failure to abide by the acceptable use policy can result in disciplinary action, including termination.
- Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Company's information assets or resources.
- Violations of the rights of any person or Company by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of 'pirated' or other software products that are not licensed for use by the Company.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or the end-user does not have an active license are strictly prohibited.
- Using a Company's computing asset to procure or transmit material that actively violates sexual harassment or hostile workplace laws.
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Making fraudulent offers of products, items, or services originating from any Company account.

- Sending unsolicited email messages, including the sending of 'junk mail' or other advertising material to individuals who did not specifically request such material (email spam).
- Providing information about, or lists of, Company's employees to parties outside the Company.
- Solicitation of email for any other email address other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding 'chain letters', 'Ponzi', or other 'pyramid' schemes.
- Blogging or other publication by employees about employees or Company's business interests, whether using Company's property and systems or personal computer systems, is not permitted without explicit management authorization.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
- Using removable media (including personal USB sticks, SD cards, or external hard drives) not provided by the Company.

Mapping with Industry Standards

This policy addresses the following risks related to Acceptable use of assets and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Loss of CIA (confidentiality, Integrity and Availability)	5.10 Acceptable Use of Information and Other Associated Assets 5.14 Information Transfer
Non-adherence to the laws and regulations and Compliance	5.14 Information Transfer
Unauthorized access	5.10 Acceptable Use of Information and Other Associated Assets
Information Leakage	5.10 Acceptable Use of Information and Other Associated Assets 5.14 Information Transfer
Theft	5.14 Information Transfer
Physical Loss or damage	5.10 Acceptable Use of Information and Other Associated Assets 5.14 Information Transfer

Enforcement

The Acceptable Use Policy is enforced by management alongside the information security team. All exceptions to the policy should be brought to the attention of management and/or the information security team.

Non- Compliance

Violations of the policy may subject employees to disciplinary action, including removal of privilege to the systems, up to and including termination of employment. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable Veranda Learning policies.
- Termination of employment.
- Legal action according to applicable laws and contractual agreements.

Validity and Document Management

The owner of this document is the management, who must check and, if necessary, update the document at least once every 12 months.