Device Policy Template

Why do schools require a device policy template?

Use of mobile devices are quickly replacing rote learning and other traditional methods of teaching. It helps foster an active learning environment where students can easily exchange ideas, get quick feedbacks and get instant access to all materials they need to complete their lessons.

Implementing a device usage policy can resolve some of the issues educational institutions may have regarding administrative difficulties in managing the devices. It also helps take care of distractions students may come across when using these devices such as the urge to access social media sites and responding to text notifications during lessons.

This customizable policy template comes with most of the basic requirements your institution needs in administering a device usage policy that secures devices and data and sets restrictions to prevent the occurrence of any data breaches. The use of a Unified Endpoint Management (UEM) solution helps school IT admins to automate a variety of mundane tasks and ensures the devices are adequately protected from security risks and other threats.

Table of Contents

_____<Institution Name>_____: Device Policy

1. Introduction

Mobile devices play an important role in improving the learning experience of students. It helps improve critical thinking, creativity and collaboration needed to prepare students for the future. This device usage policy sets the guidelines for the secure usage of devices owned/issued/approved by _____<Institution name>_____ and ensures students and staff members continue to have access to the school's resources throughout the day.

2. Scope

This policy is applicable to all students and staff members with access to _____<Institution name>_____ resources, networks, data and systems.

3. Policy

3.1. Acceptable use

Devices shall only be used in accordance with the administrative and educational purposes of _____<Institution name>_____. Their usage should be strictly aligned with the guidelines set forth by school personnel for the use of devices within the school property and for other school related activities.

The devices should be well equipped to support learning activities in and beyond classrooms. A list of approved devices can be sought from the _____<School Administration>_____.

All end users, which includes students and staff members must take complete ownership of their respective devices and sign _____<Institution name>_____ _____<Acceptable Use Agreement>_____ prior to connecting the devices to the school's network.

The devices shall be subjected to periodic and regular monitoring via a Unified Endpoint Management (UEM) software. This would help the _____<IT Team>_____ set adequate number of restrictions on the devices to protect all information processed and managed by these devices.

Personally owned devices should be registered with the _____<School Administration>_____ for approval.

Any personal devices brought into the school premises shall be done at the risk of the owner. _____<Institution name>_____ shall not be held liable for any damages resulting from the use of such devices within the school. The school shall not be held accountable for any device malfunction resulting from any unauthorized changes made to the device while on school network.

_____<Institution name>_____ recommends end users make their devices identifiable with the use of distinctive device IDs. Passcodes and PINs shall be remotely set up via a UEM solution to aid in security. Users should agree to never disclose their passwords to anyone.

The devices are strictly forbidden from being used during tests and exams until a written approval has been obtained from the _____<Department Head/School Administration>_____. The devices shall be locked down with minimum features to function to preserve the purpose for which the tests/exams are being carried out and to restrict students from accessing materials online. The devices should be used solely in accordance with the _____<Exam Supervisor>_____'s directions.

3.2. Access Control

The _____<IT Team>_____ shall maintain the right to permit or deny connecting mobile devices to school networks. The _____<IT Team>_____ has the complete right to disenroll devices that can put the _____<Institution name>_____'s systems, data and users at risk.

Devices may only access _____<Institution name>_____'s network and data using a Secure Socket Layer (SSL) and Virtual Private Network (VPN). VPN settings shall be configured with the help of a UEM solution.

_____<IT Team>_____ reserves the right to restrict users from needlessly transferring information within the school network. Audit trails shall be maintained to detect the presence of any possible data breaches and misuse.

User access to _____<Institution name>_____ network shall be monitored on a regular basis to identify unusual activities.

Strict access controls would be maintained on the devices based on the requirements of the user.

Exit processes would be maintained when an employee leaves the company. This would include deprovisioning the device, revoking the link between the UEM software and the device, removing access to all school resources and securely deleting all sensitive information.

3.3. Data protection and device security

Data protection and being in compliance with various regulations applicable to _____<Institution name>_____ is one of our top priorities. _____<IT Team>_____ shall ensure all devices managed by _____<Institution name>_____ stays updated by rolling out OS updates, app and security updates when necessary.

Changing any of the device settings is strictly forbidden. Restrictions shall be placed to dissuade users from making any unauthorized changes to the device settings. This is done to preserve the privacy rights of users and to protect the confidential and proprietary nature of information passing through the school's networks.

The software and applications approved and installed by _____<Institution name>_____ should remain in the managed devices and be accessible at all times. Periodic checks shall be conducted by the _____<IT Team>_____ to make sure the required applications are not removed. These applications shall be considered mandatory as it would aid in various learning activities and help carry out the smooth functioning of _____<Institution name>_____'s daily administrative operations.

Apps added by _____<Institution name>_____ shall remain the property of the school and will not be accessible to students once they leave _____<Institution name>_____. Apps bought by the user for their own personal use shall remain theirs even after they leave the school.

Data shall be monitored to ensure that critical educational and administrative activities shall not be impacted with the increased number of connected devices to the school's network.

Pictures and videos shall only be taken within school premises with prior permission.

Staff is discouraged from using the device for personal purposes during teaching sessions.

_____<Institution name>_____ shall maintain a list of approved devices and application. This list shall be made available to students and staff.

Users who wish to connect school owned devices to networks outside of _____<Institution name>_____ scope, should have a personal firewall pre-approved by _____<Institution name>_____ enabled within the device. Other security measures deemed necessary by _____<Institution name>_____ shall be enabled on the device as well.

Confidential data should not be stored on devices that fails to meet the standards set by _____<Institution name>_____.

Anti-virus and anti-malware software shall be kept up to date to adequately protect the device.

Encryption shall be remotely enabled on the device to ensure data protection. In personal devices, a separate encrypted space shall be maintained to store all resources and materials related to _____<Institution name>_____. Users should make certain confidential data is not stored within unencrypted space of the device.

All hardware security configurations in personal and school owned devices should be pre-approved by _____<Institution name>_____ _____<IT Team>_____.

3.4. Data disposal

Students and staff members should follow _____<Institution name>_____ approved data removal procedures to delete school specific data from devices when no longer required.

3.5. Guidelines on Internet and email usage

Use of well-known social media and text messaging platforms are not permitted without prior approval from the _____<Department Head/School Administration>_____.

End users shall be held personally accountable for what they post and are advised to refrain from posting any confidential, proprietary information on a social site. Online discussions on _____<Institution name>_____'s employees (full and part-time), vendors, clients and partners should not be held without written authorization from concerned authorities.

Comments that are racist, sexist and homophobic in nature shall not be tolerated. End users found to make comments of this nature shall be immediately expelled or terminated.

Web filtering shall be applied to block access to websites not approved by _____<Institution name>_____. A UEM solution shall be used to manage access to the whitelisted websites. This is done solely to improve the learning experience of users. Users can reach out to the _____<IT Team>_____ or _____<Department Head>_____ to address any concerns they may have regarding privacy rights.

Use of internet for personal usage shall only be permitted before class and during breaks. If any urgent communication needs to be done, they shall be done with the written approval of the _____<Department Head/School Administration>_____.

_____<Institution name>_____'s network and email systems should not be used for personal business purposes.

Downloading of video, music files, games and other software for non-study and work-related purposes is strictly forbidden.

The school shall keep records of the internet traffic to protect _____<Institution name>_____ and its staff from various security breaches.

Any reported instances of cyber-bullying shall lead to immediate expulsion. _____<Institution name>_____'s email systems should not be used to harass or bully any students or staff members.

During working hours, the internet can only be accessed for purposes related to research, education, outreach and for carrying out other administrative tasks.

Various data loss prevention policies shall be put in place to protect the transfer of information passing through _____<Institution name>_____'s networks.

3.6. Communication

Communication between personnel within _____<Staff members>_____ and students shall only be held via school issued email accounts. Unauthorized communication between a personnel and students are strictly prohibited. This includes, but not limited to:

- Calls
- Texting
- Use of messaging services
- Communication through personal email and social networking accounts

Should communication be done outside of school issued email accounts, the administration should be notified of the communication and its purpose. Approval should be maintained before such communication is made.

3.7. Viruses and malware

Users are instructed not to install any files or media infected with virus into their systems. Oftentimes, these files get downloaded within the system without users being aware of it. In order to ensure the files accessed are virus free, users should restrict downloading work related files from unsecure areas of the internet. Users should be cautious when receiving mails from unknown sources. Before placing any files on _____<Institution name>_____'s network, users should scan it for viruses using a virus scanning software.

3.8. Lost or stolen devices

In case if a user loses a device or reports it stolen, they should immediately notify the _____<School Administration>_____ and _____<IT Team>_____ of it.

For school owned devices, a full device wipe will be initiated whereas in personal devices, a partial wipe or a corporate wipe will be initiated where only school specific information will be deleted.

The device will be locked to ensure no one other than members of the _____<IT Team>_____ accesses it.

As soon as the device is discovered, it should be given to _____<IT Team>_____ for re-provisioning.

3.9. Reporting of information security incidents

Users must report to members of the _____<IT Team>_____ or the _____<School Administration>_____ if any incidents or suspected incidents of unauthorized data loss or access to networks, databases or resources are detected.

3.10. Breach of policy

End users cannot access school resources without agreeing to the terms and conditions stated within this policy. If users have any questions regarding this policy, they should be free to contact _____<IT Team>_____. Failure to comply with this policy may result in the suspension of all device usage and connectivity privileges.

The _____<School Administration>_____ shall be notified of any breaches to the policy and shall be responsible for the carrying out the appropriate disciplinary action.