Personal Device Policy

Salem Academy and College grants authorized employees the privilege of purchasing and using smartphones, tablets, and laptops of their choosing for work purposes for their convenience. Salem reserves the right to revoke this privilege if users do not abide by Institutional policies and procedures.

This policy is intended to protect the security and integrity of Salem's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Salem employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the Salem network.

Devices and Support

- Smartphones including iPhone, Android, Blackberry, and Windows phones are allowed.
- Tablets including iPad and Android are allowed.
- Laptops including MacBooks, Windows, Chromebooks, and GNU/Linux are allowed.
- Connectivity issues are supported by Salem Information Technology (IT); employees should contact the device manufacturer or their carrier for operating system, software, or hardware-related issues.
- Before employees can access the network with personal devices, devices must be presented to IT for proper configuration of standard apps, such as browsers, office productivity software, and security tools.

Reimbursement

- Salem will not reimburse employees for any portion of the cost of personal devices, roaming, plan overages, etc.
- Salem will not pay an allowance, cover the cost of a phone/data plan, etc., unless Salem provides a device to an employee while retaining ownership of the device. In these cases, Salem will only cover the cost of the phone/data plan and/or any apps required by the job function of the user. Users must receive prior written approval from Salem IT for the purchase of such apps.

Security

- In order to prevent unauthorized access, personal laptops or other electronic devices must be protected with a strong password and lock if idle.
- Personal laptops must have anti-virus/anti-malware protection installed. Employees are responsible for providing this software, as well as paying for any subscription or purchases incidental to the installation of said software.
- Salem-owned software is not available for installation on personal laptops.

- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Employees are encouraged to use Salem-owned devices for work with student data and other Institutional data that is subject to confidentiality and data security protections. If employees use personal devices for this purpose, Salem reserves the right to manage this data in conformance with applicable data security laws, regulations, and policy.
- Personal laptops and other electronic devices not allowed to connect to the employee-only portions of Salem's network (e.g., Salem Employee Wi-Fi Network).
- Salem-managed data used on personal devices may be remotely rendered inaccessible for security purposes if 1) the device is lost, 2) at separation of employment, or 3) IT detects a data or policy breach, or a virus or similar threat to the security of Salem's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- While IT will take precaution in trying to prevent personal data from being lost in the event it must remotely deny access to Salem data on personal devices, , it is the employee's responsibility to take additional precautions, such as backing up personal email, contacts, etc.
- Salem reserves the right to disconnect devices or disable services without notification.
- Lost or stolen personal devices used for work purposes must be reported to the Director of Information Technology within twenty-four (24) hours of the incident.
- When using personal devices for work purposes, employees are expected to do so in an ethical manner at all times and to adhere to the Standards for Acceptable Use of Electronic Resources.
- Employees are personally liable for all costs associated with their personal devices.
- By opting to use their personal devices for work purposes, employees assume full liability for risks including, but not limited to, the partial or complete loss of Institutional and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Salem reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Please refer to the MySalem Intranet at Information Technology for the most current version of Institutional policies related to the use of Electronic Resources and other technology-related support.