BRING YOUR OWN DEVICE (BYOD)

POLICY

Risks, Liabilities, Disclaimers

Employees who elect to participate in bring your own device (BYOD) accept the following risks, liabilities and disclaimers: At no time does the Sherman College accept liability for the maintenance, backup, or loss of data on a personal device. It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems before requesting assistance from Sherman Information Technology department.

- Persons violating this policy may also be held personally liable for resulting damages and civil or criminal charges. Sherman College will comply with any applicable laws regarding data loss or breach notification and may also refer suspected violations of applicable laws to appropriate law enforcement agencies.

- The Sherman College shall **NOT** be liable for the loss, theft, or damage of personally owned computing device (POCD). This includes, but is not limited to, when the device is being used for Sherman College business, on Sherman College time, or during business travel.

- Sherman Information Technology department provides only limited security for the Sherman Guest network and at no time does the Sherman College accept liability for the security of a POCD.

- Sherman Information Technology department will maintain wise financial stewardship of Sherman College's resources by assessing the employee's usage of a POCD in proportion to their usage of Sherman College provisioned computing device. Sherman Information Technology department, at its discretion, may elect to discontinue providing a Sherman provisioned computing device if it is no longer reasonably needed.

- Sherman Information Technology department reserves the right to implement technology such as Mobile Device Management to enable the removal of Sherman College owned data.

- POCD may be subject to search and review as a result of litigation that involves the College.

User Responsibilities

Employees who elect to participate in BYOD must adhere to this policy and all Sherman College policies while using a POCD device on a Sherman College Network.

Employees who elect to participate in BYOD must:

- Not store Sherman College personally identifiable information data on personally owned computing devices.

- Destroy, remove or return all data, electronic or otherwise belonging to Sherman College, once their relationship with Sherman College ends or once they are no longer the owner or primary user of the POCD. (E.g. the sale or transfer of a POCD to another person)

- Remove or return all software application licenses belonging to Sherman when the POCD is no longer used for Sherman College and notify Sherman security of any theft or loss of a POCD containing data or software application licenses belonging to Sherman

- At no time may a POCD be connected to the secure Sherman networks (E.g., Sherman Wireless SSID) without prior approval.

Devices and Support
In general, any computing device may be connected to the Sherman Guest wireless SSID network provided its use does not disrupt any Sherman College computing. Sherman Information Technology department will prioritize the support of Sherman owned computing devices and production information systems and provide only limited support for POCD. Limited support for POCD is defined as:

POCD support for both the Sherman Guest wireless SSID network:

- Maintaining the availability of the Sherman Guest wireless SSID network

- Maintaining the availability of the authentication systems for the Sherman Guest wireless SSID network.

- Verifying authentication credentials are valid.

Additional POCD support for the Sherman College network only:

- Troubleshooting connectivity or authentication issues on POCD.

- Configuration of POCD for communication with Sherman College email system (e.g. Exchange ActiveSync).

- Configuration of VPN and/or Remote Desktop access to Sherman College computing resources.

- Providing software application support when reasonably possible as determined by Sherman Information Technology department. Note: It is the responsibility of the device

owner to have and provide authentic, individually owned and registered software before any assistance will be provided.

- Ensuring wireless network compatibility for officially supported device types. Sherman Information Technology department will strive to ensure compatibility for all major devices according to market share. Should you have any concerns regarding compatibility, please consult with Sherman Information Technology department prior to purchasing any devices you intend to use on the Sherman Guest network.

Examples of POCD support not provided include, but are not limited to:

- Troubleshooting device performance or hardware problems
- Troubleshooting software applications or cloud services
- Installing OS upgrades, OS patches, or Sherman College owned software on POCD
- Backing up device data or migrating data to a new device
- Removing malware or spyware

Security
Currently, no security restrictions or Mobile Device Management (MDM) solutions have been implemented for the Guest or Sherman networks. However, the Information Technology department reserves the right to implement such restrictions or solutions.

Sherman's Information Technology department may perform security scans against any personally owned device that accesses Sherman networks. Sherman's Information Technology department may, without notification, prevent or ban POCD which disrupt any Sherman College computing resources or are used in a manner which violates any Sherman College policies.

Exclusions or Special Circumstances
Exceptions to this Policy shall only be allowed if previously approved by the director of information technology and this approval is documented and verified.

Consequences
Use of College electronic information resources contrary to this policy or applicable federal, state or local law is prohibited and may subject the user to disciplinary action including, but not limited to, suspension of the user's access to the electronic information resources. Users also should be aware of other possible consequences under college policies and federal, state, or local laws, particularly those related to computer crime and copyright violation.

Recourse/Appeals
If a department or individual feels that actions taken under this policy have been inappropriate, a review of the decision may be requested. The review will be conducted by the provost and executive vice president. If, after the review, there is still a disagreement with the decision, appeals should be directed through the existing procedures established for employees and students.