I. Introduction:

In response to the increasing use of personally owned computing devices (POCD) by employees for ACOM business purposes, ACOM has established an official bring your own device (BYOD) policy. The purpose of this policy is to define the appropriate use and procedures for using personally owned computing devices with ACOM Information Technology and Information System resources.

II. Applicability:

This policy applies to any user who makes a wired or wireless network connection from a POCD to ACOM Information Technology and Information Systems resources (ie, SharePoint, LCMS+, E-Value, Email, etc) and the "ACOM_Guest" or "ACOM_Staff" or "ACOM_Students" network.

BYOD is a rapidly changing technology and ACOM reserves the right to modify this policy, including eliminating all support for BYOD, at any time. ACOM IT may elect to implement additional requirements or processes to safeguard the College's Computing Resources (e.g. mobile device management (MDM), enforcing separation of ACOM data from personal data, remotely removing ACO data, additional registration processes, or requiring a PIN number to access systems). The most current version of this policy will be posted on Information Technology's SharePoint website.

III. Policy Statement:

In order to support the BYOD model while appropriately managing ACOM's risk, the following policies are established.

Risks, Liabilities, Disclaimers

Employees and Students who elect to participate in BYOD accept the following risks, liabilities and disclaimers:

- At no time does the 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 IT.
- Persons violating this policy may also be held personally liable for resulting damages and civil or criminal charges. ACOM 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 College shall **NOT** be liable for the loss, theft, or damage of POCD. This includes, but is not limited to, when the device is being used for College business, on College time, or during business travel.
- ACOM Information Technology provides only limited security for the ACOM Guest and ACOM Staff networks and at no time does the College accept liability for the security of a POCD.
- ACOM Information Technology will maintain wise financial stewardship of the College's resources by assessing the employee's usage of a POCD in proportion to their usage of ACOM provisioned computing device. ACOM IT, at its discretion, may elect to discontinue providing a ACOM provisioned computing device if it is no longer reasonably needed.
- ACOM Information Technology reserves the right to implement technology such as Mobile Device Management to enable the removal of ACOM owned data.

- Usage of ACOM Information Technology and Information Systems resources on POCD constitutes the understanding of a no privacy environment.
- POCD may be subject to the 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 College policies while using a POCD device on a ACOM Network. In particular, the ACOM *Code of Conduct Policy* available on the ACOM website and the ACOM *Security for Information, Computing and Network Resources Policy* and the *Information Technology Usage Policy* available on the Information Technology (IT) website must be followed.

Employees who elect to participate in BYOD must:

- Not store ACOM data on personally owned computing devices
- Destroy, remove or return all data, electronic or otherwise belonging to ACOM, once their relationship with ACOM 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 ACOM when the POCD is no longer used for ACOM Business
- Notify ACOM Information Systems of any theft or loss of a POCD containing data or software application licenses belonging to ACOM

Devices and Support

In general, any computing device may be connected to the ACOM Guest networks provided its use does not disrupt any ACOM Computing Resources or violate the *Network and Computer Usage Policy*.

Information Technology will prioritize the support of ACOM owned computing devices and production information systems and provide only limited support for POCD. Limited support for POCD devices is defined as:

POCD support for both the ACOM Guest networks:

- Maintaining the availability of the ACOM Guest networks
- Maintaining the availability of the authentication systems for the ACOM Guest networks.
- Verifying authentication credentials are valid.

Additional POCD support for the ACOM network only:

- Troubleshooting connectivity or authentication issues on POCD.
- Configuration of POCD for communication with ACOM Email system (e.g. Office365).
- Configuration of VPN and/or Remote Desktop access to ACOM Computing Resources.
- Providing software application support when reasonably possible as determined by IT. 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 as listed on Information Technology's website. IT will strive to ensure compatibility for all major devices according to market share. Should you have any concerns regarding compatibility, please

consult with Information Technology prior to purchasing any devices you intend to use on the ACOM 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, 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) solution have been implemented for the ACOM Guest networks. However, ACOM Information Technology reserves the right to implement such restrictions or solutions.

ACOM IT may perform security scans against any personally-owned device that accesses ACOM networks in accordance to the ACOM *Network and Computer Usage Policy*. IT may, without notification, prevent or ban POCD which disrupt any College Computing Resources or are used in a manner which violates any College policies.

ACOM IT has the ability to do a selective wipe to remove only organizational information, or a full wipe to delete all information from a POCD and restore it to its factory settings.

- Full Wipe: Deletes all data on a user's POCD, including installed applications, photos, and personal information. When the wipe is complete, the device is restored to factory settings.

- Selective Wipe: Removes only organization data and leaves installed applications, photos, and personal information on a user's POCD.

When the device is wiped, the device is removed from the list of managed devices. ACOM reserves the right to perform as Full and Selective Wipe. There are several reasons for wiping devices:

- Mobile devices like smartphones and tablets are becoming more full-featured all the time. This means it's easier for users to store sensitive information (such as personal identification or confidential communications) and access it on the go. If one of these mobile devices is lost or stolen, wiping the device immediately can help prevent ACOM's information from ending up in the wrong hands.

- When a user leaves the organization with a personal device that is enrolled in MDM for Office 365, ACOM can help prevent organizational information from going with that user by doing a selective wipe.

- If ACOM provides mobile devices to users, ACOM may need to reassign devices from time to time. Doing a full wipe on a device before assigning it to a new user will ensure that any sensitive information from the previous owner is deleted.

It is not ACOM's intent to wipe phones and delete users information. ACOM IS will not intentionally wipe users phones without direct instruction from Dean of ACOM or users.

Reimbursement

Any reimbursement claim for purchases associated with personally owned computing devices is subject to the ACOM Computer Technology Acquisition Policy and the Reimbursement Policy and Procedures for College-Related Business Expenses which can be found in the ACOM Faculty and Staff Handbook. Furthermore:

- Computer technology purchased for personal use will not be reimbursed by the College.
- Computer technology purchased with personal funds, regardless of the intended use, may not be reimbursed by the College, without prior approval by Information Technology and Finance and Administration. This includes, but is not limited to, software or technology services, including repair or technical support services.
- Loss, theft, or damage to personally owned computing devices will not be reimbursed by the College.

IV. Enforcement

Suspected violations of this policy will normally be handled through ACOM disciplinary procedures applicable to the relevant user. ACOM may suspend a user's access to the ACOM Guest network, or any College Computing Resources, prior to the initiation or completion of such disciplinary procedures, when it reasonably appears necessary to preserve the integrity, security, or functionality of College Computing Resources or to protect ACOM from liability. ACOM may also refer suspected violations of applicable laws to appropriate law enforcement agencies.

The College's Director of Information Systems shall be the primary contact for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any legal issues concerning the policy shall be referred to the appropriate officials for advice. Employees may appeal the resolution of problems in regards to this policy via the College's Conflict Resolution Policy.

Approved Dean's Cabinet – August 2017

Last Updated – June 21, 2018