Cary Institute of Ecosystem Studies Bring Your Own Device (BYOD) Policy
February, 2019

In many organizations, staff choose to use their personal technology (laptops, phones, tablets, etc.) for work, or to connect their personal devices to institutional networks. In the event that a staff member wishes to use a personal device in this way they may do so in accordance with this policy and its related procedures.

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

The policy also enables the Cary Institute to assist the staff member in the appropriate management of their device and personal data although such management will be considered an incidental benefit of compliance and not the driving force behind this policy.

The Cary Institute reserves the right to revoke the privilege of using a personal device for work purposes if users do not follow the policies and procedures outlined below.

Cary Institute employees must sign below and agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the Institute network. All signed policies should be returned to the Human Resources office.

Acceptable Use

- All Cary Institute policies and procedures related to use of technology apply to employee devices that are used on Cary Institute networks and systems.
- Devices may not be used on the Cary network to:
    - Download, store, or transmit illegal information or data.
    - Harass, discriminate, or retaliate against others.
- Texting, emailing or speaking without a hands free device while driving is illegal in most states. Employees must adhere to the laws of the states in which they are driving Cary Institute-provided vehicles.

Devices and Support

- Smartphones using the iOS (Apple), Android, and Windows Phone operating systems are allowed.
- iPads, Android tablets, and Windows tablets are allowed.
- Other smartphones, tablets, and personal laptops will be allowed on the network on a case by case basis by the IT Manager. Any device that is not approved for network use will be reviewed by executive management.
- Connectivity issues are supported by IT.

Security

- In order to prevent unauthorized access, devices should be password protected using the features of the device.
- The employee will immediately notify IT when a device containing Cary data, including network login information, is lost or stolen or when there has been a data breach.

- The employee's device may be remotely wiped in only extreme situations and may happen if (1) the device is lost; (2) IT detects a data or policy breach, a virus or similar threat to the security of the Cary network.

Risks/Liabilities/Disclaimers

- The Cary Institute will take every precaution to prevent the employee's personal data from being lost in the unlikely event it must remotely wipe a device.
- It is the employee's responsibility to take additional precautions, such as backing up personal email, contacts, and all important data. The Cary Institute highly recommends regular cloud or computer-based backups and will advise, as time permits, on strategies to secure information on your personal device.
- The Cary Institute reserves the right to disable Cary account features (Gmail, Calendar, Drive, etc.) without notification. Every attempt will be made to contact the employee first to inform him/her of what needs to be done but if instructions are not followed, the Institute may have to take action. The IT manager will get the approval of executive management if steps need to be taken and the employee has not acknowledged contact.
- Employees are expected to adhere to the Cary Institute's Computer Use Policy while using their devices on the network. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Cary Institute 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.
- In the event of litigation or investigation (internal, criminal, audits), Cary Institute may be required to and reserves the right to access Cary Institute data stored on the device.

Nothing in this policy will in any way limit Cary Institute's (i) rights to enforce any of its workplace policies and procedures or (ii) obligations to comply with applicable laws.

___ I *do wish* to use my personal device(s) for work-related purposes

___ I *do not wish* to use my personal device (s) for work-related purposes

---

I understand that by signing below I accept and agree to abide by the terms and conditions set forth in this policy.

Employee (Print Name):

Employee (Signature):

Date:
