**Faculty and Staff FAQs: Telecommuting, Data Protection and Privacy, Canvas, and Zoom**

**TELECOMMUTING:**

**Are there guidelines for telecommuting?**

Yes. BC High has implemented a telecommuting/work from home policy and guidelines intended to assist departments and employees in interpreting and implementing the School’s Telecommuting Policy. You can access the policy [here](https://bchigh.myschoolapp.com/ftpimages/225/download/download_4394321.pdf?_=1596839876967).

**Will BC High provide office supplies necessary to complete my work assignments?**

Yes. Office supplies necessary to complete work assignments should be obtained during the teleworker’s in-office days. The teleworker will not be reimbursed for supplies normally available in the office. The employee must have prior approval from their manager for the purchase of any supplies that cannot be obtained through normal supply channels. Without prior approval, such purchases will not be reimbursed. Any School materials taken home should be kept in the designated work area at home and not be made accessible to others.

As a general rule, confidential and/or proprietary information may not leave the School premises. Confidential materials shall not be taken from the School without advance notice from your department manager. If it is necessary for data to be downloaded or transported to be used off-site, employees must have the approval of their manager and inform them of the methods being used to safeguard the information.

Confidential materials include documents that contain PII, student transcripts, student files etc.

**Does the clean desk policy apply to telecommuting?**

Yes. Employees are prohibited from leaving papers, notes, post-its or any other documents that contain Personally Identified Information (PII), sensitive information, and/or log-in credentials (usernames and passwords) to accounts that contain access to sensitive or personal information unattended and/or out in the open and in plain view on their desk, keyboard, work area, and/or in a common workspace, copier, and/or printer. This applies while telecommuting as well.

**What is Personally Identifiable Information (PII) and sensitive information?**

Massachusetts law requires that anyone storing personally identifiable information (PII) on a desktop, laptop, thumb drive or other media (including paper) take special precaution to protect this information.

PII is a specific category of particularly sensitive data defined as follows:

Information that includes a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

* Social Security number (SSN).
* Financial account numbers such as bank account numbers, student loan records, credit card number, or debit card number with or without any required security code, access code, or password such as expiration date or the individual’s mother’s maiden name that could permit access to an individual’s financial account.
* Driver’s license number or state-issued / government issued identification number.
* Medical information (any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis provided by a licensed health care professional).
* Health insurance information (an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records).
* Student education records (including grades and disciplinary records).

More information regarding Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth is available [here](https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-ma-residents).

**How do I check my laptop for malware?**

Every endpoint has Sophos Advanced and Intercept X installed on their device. All employees are responsible for keeping their Sophos software up to date and when asked, must respond quickly to requests from the IT Department to take action on their machine. If you have any questions or concerns, you can contact the IT Team at ITDepartment@bchigh.edu.

**Do I need to secure my home Wi-Fi network?**

Yes. Your router controls access to your home Wi-Fi network and subsequently access to all devices that are connected to it. If someone gains access to your router, they may be able to compromise your devices, including your BC High owned device and the data stored inside.

**How can I secure my home Wi-Fi network?**

Below is a “step-by-step” guide for securing your home Wi-Fi network. If you have any issues in following these steps, please contact our IT team at ITDepartment@bchigh.edu for further assistance.

* Change the password required to access your router settings, as many people just leave the defaults in place, leaving your router open to reconfiguration. Every wireless router is delivered out of the box with a default username and password, which is needed to install and connect your router. This makes it easy for hackers to guess it, especially if they know the manufacturer. The router or admin password is used to log in to the router’s web-based setup page for configuration or verification purposes.
* Change the default SSID (service set identifier) or “network name.” (at school it’s called BCHigh) This makes it harder for attackers to know what type of router you have. If a hacker knows the manufacturer’s name of your router, they will know what vulnerabilities that model has and may try to exploit them.
* Use a WPA2 (Wi-Fi Protected Access II) secured password to guard against unauthorized access to your home Wi-Fi network. This configuration is made at the router level under security.
* Use a **strong** WPA2 wireless password (also known as a network security key). A wireless password is different from the router or admin password. The wireless password is used to connect wireless devices to your Wi-Fi/wireless home network. A good wireless password should be at least 20 characters long and include numbers, letters, and various symbols.
* Require all devices to submit a password in order to connect to your network.
* Change your wireless password on a regular basis
* If you need help, your internet service provider (ISP) is the best place to start.  Here are links to Xfinity and Verizon and recommendations from CISA and the Department of Homeland Security.

**Can I use free or unsecured Wi-Fi to access the internet from my work computer?**

No. Security and confidentiality shall be maintained as it would while on site. All work should be conducted using your secured home network. If you find yourself in need of Wi-Fi outside of your secured home network, in an emergency, it is safest to use your mobile phone as a hot spot. If you have any questions, please contact our IT team at ITDepartment@bchigh.edu for further assistance.

**What are IoT devices and how do I secure them?**

Internet of Thing (IoT) devices, or any of the many things in the internet of things, are nonstandard computing devices that connect wirelessly to a network and have the ability to transmit data. Examples include printers, smart TVs, smart speakers, toys, wearables, smart appliances, smart air conditioning, smart thermostats, smart lighting, smart security, cars, pacemakers etc. IoT devices can be hacked and used to gain entry to your network and other devices on it, including your BC High laptop.

For security purposes, you should change the default password on all printers, and IoT devices in your home to unique and strong passwords. Check the manufacturers website for firmware updates. Research what types of data these devices collect, how it’s stored and protected, if it is shared with third parties, and the policies or protections regarding data breaches. Use Google to search your make and model. If you have any further questions regarding IoT devices and how to secure same, please contact our IT team at ITDepartment@bchigh.edu for assistance.

**Can I print work documents from my home printer?**

Yes. You can print documents from your work laptop to your home printer. For security purposes, however, you must change the default password on your printer and check the manufacturers website for firmware updates and upload those updates when needed.

Of important note, any printed documents that contain PII or sensitive information should be guarded against unauthorized assess, consistent with our policy regarding such materials and Massachusetts law.

**Do I need to use to use a virtual private network (VPN) to access my work documents remotely?**

Yes. A remote access VPN allows users to establish a secure connection with a remote computer network. BC High uses a VPN to allow Windows users access our network/file server from home or remotely, as if they were plugged directly into our network's servers and/or connected to our Wi-Fi. Only Window’s users that need to access the file server need to access to the VPN. Once we have finished our deployment of Box, all files will be stored there in place of the file server, so VPN access will no longer be necessary. If you are a Windows user and need help with the VPN, please contact ITDepartment@bchigh.edu.

**DATA PROTECTION AND PRIVACY:**

**Does BC High have policies in place that protect the privacy and security of confidential information?**

Yes. In connection with the School's Written Information Security Plan (WISP), the School has developed certain policies regarding the privacy and security of confidential information. Every employee is expected to become familiar with the Student Records Disclosure Policy, in addition to the information security policy(ies) that apply to his or her department. In addition, every employee is expected to adhere to the School's Document Retention and Destruction Policy. A failure to adhere to these policies is grounds for corrective action, up to and including termination. Policies can be found in the bottom right corner of the Faculty and Staff Resources Page.

**Are there technical safeguards that I need to adhere to and participate in?**

Yes. Per our WISP, the school is required to implement technical safeguards. As an employee of the school you are required to

* Adhere to our password policy and use and retain multifactor authentication on your OneLogin and O365 account.
* Use Box and share work related and confidential files appropriately.
* Work with and respond quickly to requests from the IT Department to take action on your machine regarding;
	+ encrypting your devices
	+ keeping Sophos software up to date
	+ applying OS and application updates
	+ scanning for malware
	+ reporting phishing email to @reportphishing and alerting the IT Department when you interact with a suspicious link, attachment or website
	+ reporting changes in your device’s performance or signs of malware or ransomware infestation to the IT Department e.g. slow computer, blue screen, pop ups, programs opening and closing automatically, you may be sending out SPAM, locked browser or desktop with a message about how to pay, new file extensions or names

**How do I send personal (PII) or sensitive information in an email?**

Sharing of documents that contain PII or sensitive information internally, should be done using Box. Please contact the IT Team at ITDepartment@bchigh.edu if you need help creating a shared folder.

If your role requires you to share PII or sensitive information externally over email, that communication must be encrypted. To encrypt an email, type the word ‘encrypt’ in the subject line of the email. Please contact the IT Team at ITDepartment@bchigh.edu with questions.

**Is it ok to text PII from my cell phone?**

No. Box, fax and encrypted email are the only methods allowed to transmit PII or sensitive information.

**Can I use my work email to conduct personal business?**

Messages sent via voice mail or electronic mail (“e-mail”), and the use of telephones, voice mail, computers and software provided by the School should be primarily for work-related purposes. The School permits some personal use of its IT systems, so long as this does not occur during working time and does not otherwise interfere with the Employee's productivity or School operations. Employees who do use technology provided by the School for personal purposes should be aware that information stored on the School’s voice mail, e-mail and computer systems can be retrieved and even subpoenaed for court cases. Personal or other non-approved software should not be loaded or used on School computer systems. The unauthorized downloading, copying or transmission of software, files or materials found on the Internet is prohibited. The School reserves the right to access or monitor all mediums of technology provided to employees by the School, including e-mail, voicemail, or computer, with or without notice. **Employees may not store any personally identifiable data (for example, social security numbers, drivers’ license numbers, passport numbers or copies, bank account information and health information) in their email accounts, even if that data was job related and authorized at the time it was sent or received. Please note that all employees are prohibited from forwarding School e-mails to their personal e-mail accounts.** All faculty and staff distribution lists must be used solely for School-related correspondence, and may not be used to sell items, or solicit donations for one’s self or family members. Examples include fundraisers for a child’s school or the sale of sports or theater tickets.

**Do I need to use multifactor authentication on my school email account?**

Yes. Per our Confidential Information Security Policy for all Faculty, Staff and Administration, all employees must use and retain multifactor authentication on their OneLogin and O365 accounts. If you have any questions or concerns, you can contact the IT Team at ITDepartment@bchigh.edu.

**When meeting with students, whether in person, on the phone, or virtually, with do I need to be concerned about privacy?**

Yes. All School personnel should guard against being overheard when communicating about confidential matters, should not discuss such matters in public areas, and should avoid discussing Confidential Information with others unless necessary.

**CANVAS:**

**What is Canvas?**

**Canvas** is a **Learning Management System (LMS)** designed to help faculty and students share ideas, collaborate on assignments, discuss course reading and materials, submit assignments, and much more - all online. Faculty can upload files, share feedback, engage in online discussions, or hold open office hours.

**Can I assign students homework via email?**

No. All assignments must be created in Canvas and, if necessary, submitted electronically into Canvas. When asking students for an electronic submission, please make the submission type clear e.g. Google Doc, Word Doc, PDF, ppt etc.

**Do faculty have access to G Suite and Gmail?**

Yes. Faculty are given Gmail accounts and access to the suite of Google apps upon request. As such, if teachers are working with students while using Google apps, they must use an official BC High Gmail account. Faculty can contact the IT Team at ITDepartment@bchigh.edu to obtain a Google account.

**ZOOM:**

**What is Zoom?**

Zoom is our remote learning platform, used to deliver synchronous in class and remote instruction to students.

**How do I set up a secure Zoom meeting?**

To protect against “Zoom bombings” and other cyber-attacks, all BC High classes and meetings should be restricted to authorized users only. Authorized users have an official BC High Zoom account created with a BC High email (ending either in @bchigh.edu or @students.bchigh.edu). Hosts can choose one of the authentication methods when scheduling a meeting. Meeting Authentication Options include: both bchigh.edu and students.bchigh.edu (Default), bchigh.edu, or students.bchigh.edu. **Class meetings should use the default setting.**

Therefore, all BC High employees and students are required to access/login to Zoom using their official BC High Zoom account. All meetings, by default, have the waiting room enabled and require the host to admit participants individually. It also disables the setting for allowing participants to join before host. By default, a passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included. By default, passcodes will be embedded in invite links for one-click join, without having to enter the passcode. By default, A numeric passcode will be required for participants joining by phone if your meeting has a passcode. For meeting with an alphanumeric passcode, a numeric version will be generated. If you have questions about Zoom, please email ITDeparrtment@bchigh.edu.

**Do teachers use Zoom analytics?**

Yes. We want to make sure that students are active in class.

**Can I record Zoom meetings?**

If and when you are recording a videoconference meeting, webinar, or conference call, you are required to inform all participants prior to recording. No one may secretly record a videoconference, webinar, telephone or conference call. Zoom will always notify meeting participants that a meeting is being recorded. It is not possible to disable this notification. For participants joining by computer or mobile device, the screen will display a recording notification. For participants who joined audio by phone, they will hear an audio prompt when they first join the meeting if it is already being recorded or at the time that recording is started.

Individual meetings with students should not be recorded. If you feel that you need to record a one on one meeting with a student, you will require the permission of the school principal.

**Can I record classes in Zoom?**

Yes. Classes can be recorded for student use only. Class recordings can be stored in Canvas only to be shared with students that missed class due to illness and only if specifically requested.

**What do I do with my old Zoom recordings?**

Zoom recordings will be automatically deleted after 7 days, unless you notify IT and ask for an extension.

**How do I enable Polling in Zoom?**

* To use polling in Zoom, you will need to verify that polling is activated in the settings for your meetings. You will then need to create the polls you want to use before the Zoom session. Once in the session, there will be a **Polling** option in the Zoom menu bar, and you can choose which poll to launch. See [Polling for Meetings](https://support.zoom.us/hc/en-us/articles/213756303-Polling-for-Meetings#h_92a08dc2-af68-44fe-8bdd-d2edb61b4754) for details on setting up polling for your meetings and creating new polls.

**Why can’t I see the Q&A feature on Zoom?**

* The Q&A feature is available only for Zoom webinars not Zoom meetings. Zoom Meetings are intended specifically for presenter and participant interaction, whereas Zoom Webinars are view only.

When you facilitate a discussion session in a Zoom Meeting, you can pose a question and have students use the **Raise Hand tool** to participate. The Raise Hand tool will alert you that a student has a response. More information on the Raise Hand feature is available [here](https://support.zoom.us/hc/en-us/articles/115001286183-Nonverbal-feedback-during-meetings).

**How do I present a PowerPoint on Zoom?**

* Refer to the following instructions for presenting a [PowerPoint on Zoom](https://support.zoom.us/hc/en-us/articles/203395347-Screen-Sharing-a-PowerPoint-Presentation#h_6f8bcb4d-55e1-4a42-83b4-af9b4e7fc201).

**How can I keep my slide presentation visible to students while they are in a Zoom breakout room?**

* When you move to a breakout room you won’t see the shared screen anymore. One option is to post a pdf of “reference slides” before class. Then students can look at the pdf when they are in the breakout room. One person in each breakout room could even share their pdf viewer window.

**How do I present a Keynote on Zoom?**

* Refer to the following instructions for presenting a [Keynote](https://support.zoom.us/hc/en-us/articles/201362963-Screen-Share-A-Keynote-Presentation).

**Can I use a Whiteboard on Zoom?**

* You can have up to 20 whiteboards per session and toggle between them. Refer to [Sharing a Whiteboard](https://support.zoom.us/hc/en-us/articles/205677665-Share-a-Whiteboard) for more information.

**Can I allow participants to share their screen on Zoom?**

* You can allow your participants to share their screen from the Share menu in the Zoom window. More information is available [here](https://support.zoom.us/hc/en-us/articles/201362153-Sharing-your-screen).

**How do I set up breakout groups on Zoom?**

* You can create up to 50 breakout groups per session. The limit for participants per Zoom meeting is 300 so you can distribute them all across 50 breakout groups. Refer to the [Enabling Breakout Groups](https://support.zoom.us/hc/en-us/articles/206476093-Getting-Started-with-Breakout-Rooms) instructions for more information.

**How do I set up and use pre-assigned breakout rooms?**

* Zoom allows meeting hosts the option of automatically or manually assigning meeting participants to breakout rooms. In a large class, manually assigning students to breakout rooms would take up too much class time. To save time, students can be pre-assigned to breakout rooms when you set up the meeting. More information is available [here](https://support.zoom.us/hc/en-us/articles/360032752671-Pre-assigning-participants-to-breakout-rooms).

**Can I use the same breakout groups multiple times within the same session?**

* Yes. Whether pre-assigned or assigned during a meeting, breakout room enrollment can be maintained. If you change enrollment in breakout groups, you will only be able to return users to their original groups if you had pre-assigned groups.

**How do I record my Zoom sessions?**

* When scheduling a Zoom session, you can choose to **Record the meeting automatically** either **on the local computer** or **in the cloud**. We recommend recording to the cloud unless you will need to edit the recording. Automatic recordings can be stopped or paused during a meeting. [Learn about automatic recording](https://support.zoom.us/hc/en-us/articles/202921119-Automatic-Recording)

If automatic recording was not set up, you can manually start a recording by clicking the **Record** button in the Zoom menu of the meeting. [Learn how to start recording manually](https://support.zoom.us/hc/en-us/articles/203741855-Cloud-recording#h_7420acb5-1897-4061-87b4-5b76e99c03b4)

\*Note: Local recordings will follow the host into breakout rooms, while cloud recordings will only record the main Zoom meeting room.

**Can I edit my Zoom recordings?**

* Editing of Zoom recordings through Zoom is limited to trimming the beginning and ending of a recording, directly in the player.