Deerfield Academy Technology Guidelines for International Travel

Deerfield Academy advises all students, faculty, and staff to observe the following precautions while traveling internationally. Adhering to these precautions will reduce the risk to you, your personal information, and the Academy's technology infrastructure and systems.

➢ Travel Notification Process:

Inform the Academy of your International Travel Plans. All students or employees who are traveling internationally on Academy business, or with Academy equipment, should register their travel at least two weeks prior to their departure**.** (Please note that students who are part of a trip managed by the CSGC do not need to register their travel, but should abide by all other posted precautions.) This will help us keep an eye on any suspicious activity from your account while you are traveling.

➢ Guidelines for Travel to High Cyber-Risk Destinations:

Members of the Deerfield community should be cautious when traveling to countries that have been identified as higher risk for cyber-incidents, including China, Russia, and Israel. Please read the following guidelines carefully, and reach out to ITS if you have questions.

- **Do not take your Deerfield-issued laptop with you.** If a laptop or iPad is absolutely essential, request a clean loaner device from the ITS Help Desk. Please submit your request at least two weeks prior to your travel date. This guarantees time to properly set up and equip you for your trip. Power the device off before returning to campus, and return it to the ITS Help Desk. Do not connect the device to the campus network following your trip.
- **Do not travel with an encrypted device.** The U.S. government prohibits traveling with encrypted devices to countries including Cuba, Iran, North Korea, Sudan, and Syria. Some countries, such as China, Israel, and Russia, have restrictions on the import and use of encryption tools. It is illegal to take an encrypted device to these countries.
- **Consider acquiring a burner phone for your trip.** Traveling with a burner phone will protect your personal device and your personal information, and will minimize the loss if it is lost or taken.
- **If you travel with a smart phone or tablet**, **back up and reset your device to its factory setting prior to traveling.** This will clear all personal information from the device. When you return home, your device can be restored to its previous state.
- **Do not rely on cloud-hosted** applications such as GoogleDrive, DropBox, etc. These applications are blocked by national firewalls in China and other countries. Consider taking printed copies of any important documents with you, or store copies of documents that <u>do not contain confidential or sensitive information</u> on your laptop hard drive.
- **Understand that VPN Access may be unreliable.** Some foreign nations restrict use of VPNs in their countries.
- **Minimize use of DAinfo and other Deerfield services that requires your username and password.** If at all possible, do not use these resources if you are not connected to a VPN.
- **Follow all GUIDELINES FOR TRAVEL TO LOW OR MEDIUM CYBER-RISK DESTINATIONS.**

➢ Guidelines for Travel to Low or Medium Cyber-Risk Destinations:

Before Leaving on an International Trip:

- **Consider leaving your technology at home.** Only carry devices that are absolutely essential. If a laptop or iPad is not essential, don't take it with you.
- **Make sure all operating systems and applications are updated.** Consult with the ITS Help Desk if you have questions about applying updates.
- **Bring only the data you need for your trip.** Where possible, limit the amount of data stored directly on your devices. Consider using cloud storage solutions, if you are traveling to a country that does not have restrictions on hosted platforms (see GUIDELINES FOR TRAVEL TO HIGH CYBER-RISK DESTINATIONS, above.)
- **Enable device encryption to protect your data on all devices:** Enabling full disk encryption will protect all the information on your devices should they get lost or stolen. High risk data must be encrypted if you travel with it. Some countries have restrictions on the import and use of encryption tools and your devices should not be encrypted if travel is to those countries (see GUIDELINES FOR TRAVEL TO HIGH CYBER-RISK DESTINATIONS, above.)
- **Install and test Deerfield's Virtual Private Network (VPN) Service.** Deerfield's VPN ensures that everything you send/receive is encrypted as it goes over the network. We advise you to test this service from off-campus prior to traveling.
- **Confirm you have recent backups of all devices that you take.** Backups will help with recovery should your device be lost or stolen.
- **Protect all of your devices with strong passwords**, and do not store passwords on your devices.
- **Understand how to use Deerfield's MFA login.** MFA can still be used in other countries when you have the appropriate device or codes to provide your second factor.
- **Don't leave a device at home or on campus that is logged into the network.** The chances of compromising your account are greater if you are connecting from multiple locations around the world.
- **Delete saved passwords from your browsers:** Open your preferred browser(s) and clear browsing data to delete saved passwords.
- **Set devices to "ask" before joining new wireless networks**, so you don't inadvertently connect to insecure or malicious networks.

While Traveling:

- **Always keep your devices with you.** Carry devices on the plane, train or bus, and keep them nearby, within your sight. Checked baggage can be lost, stolen, or tampered with.

- **Be careful when using public wireless networks or Wi-Fi hotspots.** Public wireless networks are not secure, and anyone could potentially see and intercept your traffic while you're connected. If you need Internet access, make sure you know what the reputable options are and only connect to them. TIP: ask the staff at your location for the correct network name before connecting.
- **Disable Wi-Fi, Bluetooth, and GPS when not in use.** This protects you from harmful connections and some types of tracking technology**.**
- **Use a VPN** (virtual private network) when you're traveling.
- **Do not plug in untrusted accessories.** Accessories that come from questionable or unknown sources can be infected with malware intended to steal your information.
- **Do not use any system or site that requires your credentials when using public computers.** Public computers such as hotel business center workstations and internet cafe computers are often poorly managed and provide minimal security protection, which puts your credentials at risk.
- **Keep track of credentials you used while on travel.** Take note of the credentials you use while traveling, i.e. which sites or services you access, and which usernames/passwords you use, so you can change them when you return.
- **Comply with local legislation,** including any official requests to inspect your devices. If this occurs, notify the ITS Help Desk as soon as possible and exercise caution when using the device afterwards.
- **Notify ITS if your laptop is lost or stolen.** Email helpdesk@deerfield.edu, or call 413-774-1444.

When you Return:

- **Before connecting to the campus network, run full antivirus scans on your devices**. The ITS Help Desk can assist you with scanning, if needed.
- **Using a trusted computer (not the one you traveled with) change all passwords used while traveling.** Whether you used them on your own device(s) or a public computer, they may be compromised.
- **Delete unneeded apps.** If you downloaded any apps specifically for your trip and no longer need them, be sure to delete them and the associated data.

With thanks to: University of California Irvine, Office of Information Technology; University of Pittsburgh, Information Technology; The George Washington University, Information Technology; Cornell University, Information Technology; Kansas State University .