# International Travel Security

## Travel Registration

In compliance with Policy 100 of Western Carolina University, faculty and staff who travel internationally on university business must complete the International Travel Approval Form

The Office of International Programs and Services (IPS) manages international travel registration. Students who travel internationally for academic purpose must complete related document specified by the Office of International Programs and Services.

## Travel Advisory

Consult the U.S. Department of State's Travel Advisories


WCU faculty and students wishing to travel abroad at the Level 1 and Level 2 countries may travel, but exercise normal or increased caution as advised by the U.S. Department of State Travel Advisory.

If a faculty member proposes to lead a program to a country with Level 3 or Level 4, the faculty member and Director of International Programs and Services will meet to discuss whether the program should go forward. Decision will be made in consultation with the Faculty-led Committee, College Dean, and the Provost's Office, as needed.

## Emergency Contact

In the event of an emergency abroad, WCU's Police Department can be reached 24 hours at +1-828-227-8911. Calls to the WCU Police Department involving international incidents are then routed to WCU incident response personnel. If you are calling on behalf of someone else, have as much information about the person(s) involved and/or incident as possible such as:

- The nature of the emergency/incident
- The current condition of the person(s) involved
- The person's affiliation (e.g., student, staff, faculty) and department
- Methods/reliability of future communication with the affected individual(s)

More information about how to handle emergency can be found here

## International Health Insurance

If you are traveling with GeoBlue Health Insurance, for questions about your medical plan, please contact:

Toll free within the U.S. call 1.844.268.2686
Outside the U.S. call +1.610.263.2847
customerservice@geo-blue.com

**Travel Tips and Resources**

- Travel Communication
  - Conduct research on cellular and data plans, coverage areas, and country dialing procedures at your overseas destination
    - Some providers have reasonable global calling plan
    - Purchasing a SIM card in country is also a reliable approach.
    - The International Dialing Guide
  - Establish regular check-in times and methods with family, friends, colleagues, and employers
  - Save emergency phone numbers: Program local emergency services, the nearest U.S. embassy/consulate, local friends/colleagues into your phone before you travel. Find contact information for U.S. embassies and consulates around the world. In an emergency, ask the embassy operator to connect you with the "Duty Officer" for assistance, including after hours
  - Keep hard copies of emergency numbers in a wallet, purse, and in your hotel/residence
- Travel Health
  - Conduct research on your destination before your travel. Review the Center for Disease Controls website.
    - Learn about food/water safety, as well as disease outbreaks that may be occurring, especially in the wake of severe storms and flooding
  - Obtain required and recommended immunizations and vaccinations
  - Be aware of local laws and regulations regarding the importation of medicine.
- Safety and Security (STEP program)
  - Register your travel with the U.S. Department of State's Smart Traveler Enrollment Program (STEP)
    - Receive breaking safety and security alerts and guidance directly from the U.S. embassy or nearest consulate
  - Review critical information regarding your destination via the U.S. Department of State's Country Information webpage
  - Consult the U.S. Department of State's **Travel Advisory webpage**
    - Country-specific information on active State Department warnings and alerts
    - Guidance related to travel to such countries
  - Review the Federal Bureau of Investigation's fact sheets for safety and security
    - For students traveling abroad
    - For business professionals traveling abroad
- Traveling with Electronic Devices
  - Ensure that you have the correct **plug adapters**

        - Review the information for plug adapters, and ensure, if necessary, you have the correct power converters
        - Consider purchasing a spare or external battery for your electronic devices
    - Assume no right to privacy at U.S. borders and points of entry
        - U.S. Customs and Border Protection officers can deny entry to the U.S. to individuals who refuse to unlock or surrender their electronic devices for inspection
    - Know what technologies, goods, and devices are subject to restrictions and export control licensing
        - If traveling to sanctioned countries or destinations that are otherwise impacted by export control restrictions
        - If traveling with encrypted devices or devices with encryption software, be aware of which countries restrict or require licenses for importation of such devices/software (e.g., Belarus, Burma/Myanmar, China, Hungary, Iran, Israel, Kazakhstan, Moldova, Morocco, Russia, Saudi Arabia, Tunisia, Ukraine)
    - Review best practices recommended by University of North Carolina General Administration
        - We are a global university and the mobility of our students, faculty and staff is dependent on the use of electronic devices, e.g., laptops, tablets, smartphones, digital cameras, etc. Our electronic devices hold personal and professional data and are pathways to data stored elsewhere, including the cloud. We risk the release of sensitive personal and university information when we travel.
        - When traveling internationally, your electronic devices may be subject to involuntary or voluntary inspection, copying of data, or seizure of your device-regardless of your citizenship or destination.
        - Best Practices
            - Travel with fewer electronic devices (laptops, e-book readers, smart/cellphones, tablets, digital cameras, etc.)
            - Travel with as little data as possible. Backup business-related data (including photos) to a secure cloud server maintained by your home institution, external drive, or disc before you travel. Personal data should be similarly replicated, perhaps using a service like Dropbox.
            - Know whether Export Control limitations are an issue for your device and data. Confer with your office of research compliance.
            - Strongly consider leaving your personal devices at home. Instead, purchase or use low-cost loaner tablets and notebooks that are wiped clean of data after travel. Also, pre-paid cellphones are widely available. Most constituent institutions have free loaner programs for university employees traveling on university business.
            - Assume that any network, such as a hotel or café wi-fi, is insecure. When using such a network, avoid accessing or entering sensitive information. Keep the security software current on electronic devices.
            - Disable any broadcast services, for example Bluetooth, wi-fi, GPS when not in use.

    - Do not leave your electronic devices unattended, even in a hotel room, or loan them to others while traveling.
    - Encrypt devices, but be mindful that some countries, including China and Russian Federation, forbid the transportation, in or out, of encrypted devices.
    - Do not lie to a government official.
    - Use unique passwords and change any passwords if used abroad. Don't rely on fingerprint verification alone.
    - Power devices down when not needed and particularly going through customs.
    - If data is privileged, such as through an attorney-client relationship, declare it to the government officer.
    - If you relinquish your device to a government official for further testing, request a receipt.
- Review the U.S. Department of State Traveler's Checklist