

## Georgetown International Academy

### Acceptable Use of Technology Agreement

At Georgetown International Academy, we strive to provide our students with the best technology tools to enhance their learning experience. By integrating technology into our educational practices, we create a vibrant and dynamic learning environment, preparing our students for success in an ever-changing world. This agreement outlines the expectations for technology use for all students, ensuring a safe and productive learning environment.

#### 1. BYOD Program for Grades 6-12

All students in Grades 6 through 12 are required to participate in our Bring Your Own Device (BYOD) program. Students must bring a personal device that meets the school's specifications and is capable of wireless internet connectivity. This program enables students to engage fully with digital content, collaborate on projects, and access educational tools throughout the school day.

#### 2. Device Requirements

Machine Type	Laptop or Tablet
<b>Platform</b>	PC, Mac, or iPad
<b>Processor</b>	<p><b>PC:</b> Any modern processor (Intel i5 or AMD Ryzen 5 or higher recommended for optimal performance)</p> <p><b>Mac:</b> Intel Core i5 or better</p> <p><b>iPad:</b> Modern A-series or M-series processor</p>
<b>RAM</b>	4 GB or higher (8 GB recommended for better performance)
<b>Hard Drive</b>	250 GB or Higher
<b>Operating System</b>	<p><b>PC:</b> Windows 10 or higher</p> <p><b>Mac:</b> MacOS 12 or higher</p> <p><b>iPad:</b> iPadOS 16 or higher</p>

	<b>Note:</b> The OS must be in English and have document-creating capabilities (e.g., Microsoft Word)
<b>Wireless</b>	Devices should support 802.11b/g/n (2.4 GHz) and 802.11ac (5 GHz).
<b>Ports</b>	2 or more USB ports (preferred) Audio in/out Built-in microphone VGA or HDMI
<b>Battery Life</b>	At least 4+ hours (4+ cell or higher)

#### Browser-only testing

In situations where test security is less concerning, students could use a standard browser, following these requirements:

Device	Operating System	Google Chrome*	Safari®	Mozilla® Firefox®	Microsoft Edge*
PC	Windows®10	Version 120 minimum	Not supported	Version 121 minimum	Version 120 minimum
Mac	macOS® 12 minimum	Version 120 minimum	Version 17 minimum	Version 121 minimum	Not supported
Chromebook	Google Chrome OS 120 minimum	Version 120 minimum	Not supported	Not supported	Not supported
iPad†† (grade 2+ testing)	iPadOS 16 minimum	Not supported	Version 17 minimum	Not supported	Not supported

### 3. Device Expectations

- **Usage:** Devices are to be used for educational purposes during class time, with the teacher's permission. Personal use is allowed only during designated times and in designated areas.
- **Confiscation:** Teachers may confiscate devices if students do not adhere to these expectations.
- **Examinations:** During exams, students must submit all personal devices to the teacher at the start of the exam period. Failure to do so may result in a grade of zero.
- **Responsibility:** Students are responsible for the security of their devices. The school is not liable for lost or stolen devices and will not conduct searches for missing items.

#### 4. Network Use Guidelines

Students must adhere to the following guidelines when using the school's network:

- General school expectations for behavior apply to online activities.
- Students must be polite and respectful in all communications.
- Freedom of speech and access to information are respected, but students are expected to seek appropriate materials.
- The following actions are prohibited:
  - Displaying, saving, or distributing offensive messages or pictures.
  - Using obscene or vulgar language. Damaging or disrupting computers, systems, or networks. Harassing, insulting, or attacking others.
  - Revealing personal information such as addresses or phone numbers.
  - Violating copyright laws.
  - Using another person's password or account without permission.
  - Trespassing in another person's files or work.
  - Wasting network resources, such as bandwidth or file space.
  - Downloading software for non-educational purposes.
  - Engaging in activities that may cause network congestion.
  - Using chat programs without permission.
  - Utilizing the network for commercial or political purposes.
  - Accessing inappropriate websites.

**Consequences for Violations:** Violations of these guidelines may result in a loss of access to technology resources and other disciplinary actions as deemed appropriate by school administration.

#### 5. Device Security and Storage

When not in use, students may store their devices in the school office for safekeeping.

Georgetown International Academy is not responsible for lost or stolen devices, and students are discouraged from leaving their devices unattended in desks or lockers.

#### 6. Antivirus Software and Device Restrictions

To ensure the safety and security of all student devices connected to the school's network, Georgetown International Academy will install Fortinet Endpoint Security antivirus software on all student devices. This software provides robust protection against viruses, malware, and other potential security threats. Please be aware of the following restrictions and requirements:

- **Continuous Operation:** The Fortinet antivirus software will run at all times on the student's device and cannot be disabled or turned off by the student. This is to ensure maximum protection and compliance with school security protocols.
- **Limited Access to Certain Websites or Content:** Fortinet may block access to inappropriate or potentially harmful websites to maintain a safe browsing environment.
- **Restricted Application Downloads:** Fortinet may prevent the installation of unauthorized or non-educational software to protect against security risks.
- **System Scanning and Monitoring:** Fortinet will perform regular scans of the device to identify potential threats and vulnerabilities, which may temporarily affect device performance.

- **Real-time Threat Detection:** Fortinet will continuously monitor the device for suspicious activity and may take immediate action, such as blocking access or quarantining files, to prevent harm.

If you experience any issues or have concerns regarding the antivirus software, please contact the IT department by emailing [techsupport@giagy.org](mailto:techsupport@giagy.org) to open a support ticket. Our team will assist you in resolving any technical difficulties. By agreeing to this policy, students and their parents/guardians acknowledge that the Fortinet antivirus software will be installed on the device, will remain operational at all times, and understand the restrictions it may place on certain activities. These restrictions are in place to safeguard the student's device and ensure a secure learning environment.

### **7. Agreement and Acknowledgment**

By signing this agreement, the student and their parent/guardian acknowledge that they have read, understood, and agree to abide by the terms outlined in this Acceptable Use of Technology Agreement. A signed copy will remain on file at the school, and another copy will be provided to the parents.

Student Name: \_\_\_\_\_

Grade: \_\_\_\_\_

Student Signature: \_\_\_\_\_

Parent/Guardian Name: \_\_\_\_\_

Parent/Guardian Signature: \_\_\_\_\_