

# Guidelines for Providing a Secure Testing Environment

## Using Galileo K-12 Online Technology

---

A secure testing environment can be created in a number of ways. The principles of creating this environment are similar to those applied to any classroom or computer lab where student use warrants limited and/or monitored access. Many districts find that the creation of a secure testing environment relies on methods and tools already in place, with little modification.

Because Galileo K-12 Online is an Internet-based service, access to the Internet is required for a computer lab or classroom in which online testing is being performed. However, the use of effective network sub-netting combined with proxy server controls is an effective method of ensuring that students are not accessing web searches or research sites during a testing session. *The methods discussed below are common and can be implemented by your District IT department.*

Here are some guidelines to assist in providing a secure testing environment:

- *Minimize student access to machine settings and the ability to start other programs during the testing session.* Denying users the ability to change system configuration during testing will minimize the risk of students compromising the effectiveness of other methods used to provide a secure testing environment. Your District IT department will be able to centralize this task.
- *Run browsers in kiosk mode.* This browser setting can be accomplished with a simple startup change and will help restrict access to undesired programs during testing sessions.
- *Deny access to non-ATI sites during the exam.* This step prevents students from using web searches during testing. Additionally, your District IT department can use this method to prevent access to chat applications and other web-based resources that may be used for sharing information during a testing session. Regular review of the proxy logs should confirm that this filtering was effective.
- *Ensure any printer connected to test center computers is in a secure/controlled environment.* This step can help eliminate the ability to easily print test items for later distribution among students who have not yet been tested.
- *Continue physical monitoring of the testing environment.* Even with the effective use of technological safeguards, a person monitoring students who are testing can greatly reduce the temptation to compromise test integrity.
- *Choose complex or tough-to-guess student login names/passwords.* The temptation to login to another student's account is present. Simple usernames and passwords (utilizing only a combination of the student name and/or birth date) are easily guessed for other students, once the format is revealed to a student in the form of their own username and password.
- *Make sure all answer sheets and test booklets are collected after the exam.* Online testing performed with an offline component such as pre-printed exam booklets may be distributed to other students taking the exam at a later time/date if not collected.