The Importance of Protecting Student Records

Confidentiality of student records is the responsibility of everyone at Appalachian State University, including faculty, staff, and students.

- Students rely on the University to protect their privacy
- Federal privacy law (FERPA) requires it
- FERPA stands for Family Educational Rights & Privacy Act

Under FERPA Guidelines, Students Have a Right To:

- **Inspect** their education records
- **Seek amendment** to their education records if believed to be inaccurate or misleading; to append a statement to their records.
- **Prevent disclosure** of their education records (except in certain specific situations)
- **Be notified** of their privacy rights under FERPA
- **File a complaint** with the US Dept. of Education concerning an alleged failure by the University to comply with FERPA

Who is Covered by FERPA?

- **Currently enrolled** students
- Any students who **previously attended** ASU at any time in the past to the extent that information gathered post attendance is directly related to the student’s attendance.
- **Applicants** (whether admitted or not) are treated as confidential according to the North Carolina Public Records Act

*NOTE: A student’s FERPA rights expire upon the student’s death*

When May Education Records Be Released?

- Written consent of the student
- Directory information
- Within the University to those with legitimate educational interest

When May Education Records Be Released WITHOUT a Student’s Consent?

- Judicial order/subpoena
- Health or safety emergency
- Parents of dependents (without consent only if parents claim the student as a dependent on most recent federal income return, and/or another exception applies)
- To another school in which the student seeks admission or intends to enroll (upon request of that school)
- Financial aid determination
- Other specified circumstances

A special thank you goes out to Barbara Krause, Debbie Race, and Rachel Serrano for sharing their expertise on FERPA and their contribution to the newsletter.


**Special Tips for Faculty**

**NEVER:**

- Use any portion of a student’s Social Security Number (SSN) or Student Identification Number (Student ID) in a public posting of grades.
- Link the name of a student with that student’s SSN or Student ID Number in any public manner.
- Leave graded tests or papers in a place where students will retrieve them by sorting through the papers of other students.
- Circulate as an attendance roster a printed class list with SSN, Student ID Numbers or grades.
- Discuss the progress of any student with anyone other than school officials with a legitimate interest and the student with out the consent of the student (including parents).
- Provide any third party with a list of students enrolled in your classes.
- Provide anyone with student schedules or assist anyone other than University employees in finding a student on campus.

---

**AppState Cybersecurity Report**

With no new significant threats to report this month, we will instead offer a few cybersecurity safety tips.

**Tip: Lock your computer screen when you leave your desk!**
You should log out of your laptop or workstation if you leave your work area. But if you are working on something important & don’t want to lose your work, just lock the screen. In Windows, use the Windows logo key + L. On a Mac, enable Hot Corners in your screen saver settings & set your computer to require a password for sleep & screensaver in Security & Privacy.

**Tip: Close your browser to erase cached passwords & logins**
Did you know that some sites keep you logged in via cookies even after you logout? After you are done with a browser in a public space, you should close the browser. This should make all session-specific cookies expire—keeping you a little safer online.

If you believe you have been a victim of a phishing attempt, please email phish@appstate.edu to report the incident.

---

Jim Webb,
Chief Information Security Officer

Oscar Knight,
Policy & Compliance Coordinator

Kevin Wilcox,
Security Operations Coordinator

Crystal Brooks,
Security Awareness Coordinator

Appalachian State University
Information Technology Services