INFORMATION SECURITY AWARENESS

Background

Young Harris College is subject to a variety of information privacy and security laws and regulations including the Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act (GLBA). These acts mandate specific restrictions and safeguards related to access, use, and disclosure of "Restricted Information."

Young Harris College's compliance with these acts is governed by the Information Security Plan and related polices. All employees must be aware of, and comply with the Information Security Plan and related polices located on YHC Connect.

What is "Restricted Information?"

The laws restrict information related to student "Education Records" and "Customer Financial Records."

- An "Education Record" is maintained by the college and contains personally identifiable information about current and former students. Education records include, but are not limited to, the following: College ID, Social Security number, DOB, financial aid, some health data, grades, test scores, and other academic work completed.
- "Customer Financial Records" include personally identifiable information about students, parents, employees, or related third-parties such as bank and credit card account numbers, income and credit histories, and Social Security numbers.

For more information on restricted information, please see the Data Classification and Protection Standard located on YHC Connect.

What are some risks with unauthorized access to Restricted Information?

Unauthorized access to restricted information can lead to identity theft and/or fraud. Following are some examples of events/actions which would permit fraudulent access to such information:

- A computer account with access to various information systems or network files is accessed by unauthorized individuals because a password was shared with other people, written on a post-it by the computer, or easily guessed.
- A user opens a computer virus via an e-mail attachment and the virus randomly distributes sensitive files via e-mail.

- Sensitive paper records are left in easy view where a visitor notes and records personally identifiable information.
- Verbally or visually sharing restricted information directly or within close distance of those without authority to receive such information.

What are some safe practices for information protection?

- Never share your password with others.
- Never post password information at your work area.
- Change your passwords on a regular basis.
- Use passwords that are difficult to guess or a password manager. Don't use personally identifiable information for a password. Do include a combination of letters and numbers in every password.
- Electronic access for employees should be kept current; access for employees who leave the department/area should be removed immediately.

Physical Access Restrictions

- Store restricted information records in a secure area.
- Protect desktop and laptops computers from unauthorized access. Log-off or lock your PC when not in use. Use a password protected screen-saver when you are away from your PC.
- Shred printed documents containing restricted information.

Safe Computing Practices

- Store College files on college servers (network drive) or Office 365 One Drive, not on desktop or laptop computers.
- If you access college resources from you're a personal computer, install and maintain current virus software on your computer, and make sure Microsoft updates are turned on.
- Never permit others to perform work under your system login credentials.

Fraud Awareness

- Recognize fraudulent attempts to obtain computer username/password or student/financial information. Never release such information over the phone.
- Educate all employees, particularly student assistants, about all security policies related to their job.
- Do not respond to e-mail messages asking you to provide or update personally identifiable information. Never open e-mail attachments from a non-trustworthy source.
- Be Mindful of Phishing Attempts: If something about the text of an email feels off, even if it seems to come from a trusted source, you should follow your gut. Ask yourself: is this the way we do business? Additional follow-up outside of email—such as a phone call—may be necessary for verification.