ITS CORNER

ISSUE 03: UNDERSTANDING PII & THE ROLE OF FERPA

Personal information is increasingly targeted by cybercriminals, making it crucial for individuals to understand what constitutes Personally Identifiable Information (PII) and how to protect it.

For students, parents, and educators, the Family Educational Rights and Privacy Act **(FERPA)** plays an important role in safeguarding sensitive information in educational settings.

WHAT IS PII?

PII, or Personally Identifiable Information, refers to any data that can directly or indirectly **identify an individual.**

PII, or Personally Identifiable Information, refers to any data that can directly or indirectly identify an individual. Examples include:

Direct Identifiers:

- Full name
- Social Security Number (SSN)
- Student ID number

Indirect Identifiers:

- Phone number
- Email address
- Date of birth
- Combinations of information that can identify a person.

In educational contexts, this information is particularly sensitive and protected under FERPA.

FERPA is a federal law designed to protect the privacy of student education records. It limits the sharing of PII without consent and ensures that students and parents have control over their data.

Key FERPA Guidelines:

1. Know Your Rights

Parents and eligible students (18+ or in postsecondary education) have the right to: Review and request corrections to education records, and opt-out of sharing "directory information" like names, photos, or honors.

2. Share Information Cautiously

FERPA requires written consent before PII in student records can be shared, except under specific exceptions such as emergencies.

HOW YOU CAN PROTECT PII

1. Be Mindful of Sharing Information

- Only share PII with trusted individuals, especially in educational or professional settings.
- Verify requests for sensitive information to ensure they are legitimate.
- Use secure channels, like **encrypted email**, if you must share PII digitally.

For more information on encrypting emails - see the previous ITS corner issue on email encryption!

2. Create Strong Passwords

- Follow password guidelines, such as using at *least 12 characters* with a mix of uppercase and lowercase letters, numbers, and special characters.
- Avoid including personal details like names or birthdays in passwords.
- Change passwords regularly (every 90 days).

3. Protect Physical Documents

- Keep physical records containing PII in secure locations at home or work.
- Shred papers containing sensitive information before discarding them.

4. Stay Alert for Phishing Attempts

- Be cautious of unsolicited emails, calls, or messages asking for personal information.
- Avoid clicking on links or downloading attachments from unknown sources.

Oklahoma City Community College

WHY IT MATTERS

PII theft can lead to identity theft, fraud, and other serious consequences. FERPA ensures that student records are protected, but safeguarding this information also requires individual vigilance.

By following these simple steps, you can play an active role in protecting yourself and others from data breaches and misuse.

For more information about FERPA and your rights, visit the U.S. Department of Education website or speak with OCCC's compliance officer.

Stay informed, stay secure!

ADDITIONAL ITS HELP

SharePoint Training

Curious about the move to SharePoint?
Contact venkatasai.simbili@occc.edu to be enrolled in the ITS SharePoint course or for additional help!

Got an IT Problem?

Your first stop is The Helpdesk located in the main building foyer behind the coffee shop. Mr. Brian W. Fugett, the Director of Technology Support Services, leads a team of trained on-demand IT professionals who can handle all your IT needs.

Previous ITS Corner Issues

Want to read previous issues of ITS Corner? Visit the OCCC ITS page!
https://www.occc.edu/information-technology/