CAPRI college hair skin massage nails

Personally Identifiable Information Security Procedure (PII)

What is Personally Identifiable Information?

Personally identifiable information (PII) is any information about an individual that can be used directly, or in connection with other data, to identify, contact or locate that person. Such information can include educational, financial, legal and employment records.

Examples of personally identifiable information:

Personally identifiable information can be anything that identifies an individual, such as a full name, an address, a home, office or mobile telephone numbers, an email address, a Social Security number or other form of national ID number, Internet Protocol address, a fingerprint or other biometric data, birthday, or age.

Protecting personally identifiable information:

Capri College employs numerous security protocols to ensure that personally identifiable information is safe and secure at all times.

Capri College's security policy involves a combination of encryption, threat protection (Sophos firewall, segregated wireless permissions, managed GFI antivirus, and regular security updates), data-loss prevention (automatic secure backups), and policy compliance. Employees must follow rules and common sense procedures regarding access to personal data.

Only collect and use information that is absolutely necessary. Never use, print, view or send Student SSNs, birthdates, or other PII unless necessary. If necessary, ensure information is secure or shredded after use.

Never send PII by email.

PII to be shredded must be in locked container until shredded.

Student data is stored in Fame program only, and is not allowed to be passed to third parties. Any printed personal info must be destroyed (shredded) after use and all print files are locked in secure area and never left out in unsecured area. All terminals with access to data are password protected (at least 9 characters, employing caps, numbers and symbols) not allowed to be used to visit social sites, and logged out when employee leaves station. Employees trusted to view sensitive data are required to sign that they follow and understand this policy and repercussions for non-compliance. If it is determined that an employee did not follow this policy, it is grounds for termination or criminal prosecution, depending on the specific actions and intent. If privacy breach occurs or is suspected, employee must inform management immediately.

Credit Card Policy:

- It is against Capri Policy to store credit card numbers on any document, computer, server, or database. This includes Excel spreadsheets.
- Valid ID must be presented for use of credit card.
- Email is not an approved way to transmit credit card numbers.
- Fax transmittal of cardholder data is permissible only if the receiving fax is located in a secure environment and the credit card # is not visible.
- Paper receipts including PII or credit card # must be destroyed so that account information is unreadable and cannot be reconstructed.
- Regularly update anti-virus software, Java and Adobe.
- Do not use vendor-supplied defaults for systems passwords and other security parameters.
- Each computer with any sensitive information or access to Administrative network must be password protected (9 characters, employing caps, numbers and symbols).

All Capri College employees that have access to PII must sign here:

I have read and clearly understand these policies.

____ ________________

Name ***Date***