BRIDGEVALLEY COMMUNITY & TECHNICAL COLLEGE

OPERATING POLICY

Effective Date	Subject	Number	Page
April 1, 2014	**PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)**	B-OP-17-14	1 of 7
Supersedes/Supplements:	BC A-OP-22-12		
References:	Family Educational Rights and Privacy Act (FERPA) Health Insurance Portability and Accountability Act (HIPPA)		

POLICY

Personally identifiable information (PII) is information which can be used to distinguish or trace an individual's identity. The collection, storage, and release of this information is limited and regulated by federal and state laws and regulations, such as Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPPA).

This document provides policy for the handling and protection of PII for BridgeValley Community and Technical College (College) employees and students; current, future, and alumni.

PROCEDURES

The College's Office of Information Technology is designated overall responsibility for administration of this policy.

1. It is the responsibility of the individual user to protect data to which they have access. Users must adhere to the rules of behavior defined in applicable Security Plans and College guidance.

2. Individuals who provide PII shall be notified regarding the purpose of the information, which individuals will have access to the information, how the information will be stored, how long the information will be stored, and how the information will be destroyed. The individual collecting the PII is responsible for identifying the applicable law or regulations governing the PII that is collected, and the development of the information sheet that will be made available to the individual who is providing the PII. The information sheet will be approved by the College's Chief Human Resources Officer.

3. Only PII that is required by state or federal laws or guidelines shall be collected by the College. Once collected, PII shall be protected and only released to those authorized by law.

4. PII collected in paper form shall be stored in locking file cabinets. A method of identifying files that contain PII (such as colored file folders, stamped warnings on the document, etc.) shall be used to readily identify documents that require protection from unauthorized disclosure.

5. Documents that contain PII shall not be left unattended. When in possession of a document that contains PII, the document shall be returned to the locked file cabinet as soon as the need for the document has been satisfied. While working with the document(s), every effort shall be made to ensure the safe keeping of PII and prevention of an unauthorized disclosure of the information.

6. PII collected in electronic format stored in non-volatile memory (internal or external hard drives or flash drives) shall only be processed and stored on College owned computational devices.

7. Under no circumstances shall PII be collected or stored on personal devices (such as computers, mobile devices (cell phones, tablets, etc.), storage devices, or other forms of non-volatile storage (e.g., cloud based storage such as DropBox, SkyDrive, Google Docs, etc.).

8. Under normal operational conditions, faculty and staff shall use College owned computers with a mapped drive (H-Drive, S-Drive, etc.) to store PII. When it becomes necessary to collect or create PII, and access to the mapped drive is not available, the PII shall only be stored on an encrypted College owned non-volatile device.

9. Do not send un-encrypted data that contains PII via email under any circumstances. When required to send documents containing PII via email, the file must be encrypted/password protected prior to being attached to an email message. The file shall be encrypted with a minimum encryption standard of AES-128. The password must be unique from the individual's College domain account(s). To communicate the password to the employee, it must be transmitted by one of the following methods:

   9.1. Call the employee with the password.
   9.2. Email the password to the employee in a separate email from the message that contains the encrypted document. (**Note**: Do not indicate what the password is for in the email.)
   9.3. Tell the employee in person what the password is for.

DEFINITIONS

Chief Information Officer (CIO) – The person responsible for the State's information resources. The CIO heads the IT Department and is responsible for setting and implementing the strategic plan for the College's technology infrastructure, including standards, practices, policies, and procedures.

Employees – Individuals retained and authorized on a temporary, part-time, full-time, or permanent basis by the College to perform a service. For the purposes of information technology and security policy, the term "employees" shall include, but not be limited to, the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the College to be subject to this policy. This definition does not create any additional rights or duties.

Personally Identifiable Information (PII) – As used in this policy, is information that can be used to uniquely identify, contact, or locate a single person or can be used with other

sources to uniquely identify a single individual. Appendix A details what is and what is not PII.
WEB – World Wide Web means the complete set of documents residing on all Internet servers that use the HTTP protocol, accessible to users via a simple point-and-click system (Source: wiki.answers.com).   Sometimes the “WEB” and “Internet” are used as if they mean the same thing; however, the Internet is actually the network infrastructure that supports the WEB.

BridgeValley Office of Information Technology - The Office of Information Technology, which is led by the College’s CIO and designated to acquire, operate, and maintain the College’s technology infrastructure.

Non-volatile Memory - Non-volatile memory, nonvolatile memory, NVM or non-volatile storage is computer memory that can retain the stored information even when not powered. (http://en.wikipedia.org/wiki/Non-volatile_memory, 28 Aug 2012)

Approved by: Cabinet **Date:** 4/1/2014

Appendix A: Personally Identifiable Information

Reference: http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/PROD01_008240#P46_1812
8/10/2012

What is personally identifiable information (PII)?

The term personally identifiable information refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

Examples include direct references such as name, address, social security number, and e-mail address. PII also includes any information that could be used to reference other data elements that are used for identification, such as gender, race, and date of birth.

What PII is sensitive?

Sensitive PII is defined as PII which, when disclosed, could result in harm to the individual whose name or identity is linked to the information. Further, in determining what PII is sensitive, the context in which the PII is used must be considered. For example, a list of people subscribing to a government newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII. As well as context, the association of two or more non-sensitive PII elements may result in sensitive PII. For instance, the name of an individual would be sensitive when grouped with place and date of birth and/or mother’s maiden name, but each of these elements would not be sensitive independent of one another.

For the purpose of determining which PII may be electronically transmitted, the following types of PII are considered sensitive when they are associated with an individual. Secure methods must be employed in transmitting this data when associated with an individual:

- Place of birth
- Date of birth
- Mother’s maiden name
- Biometric information
- Medical information, except brief references to absences from work
- Personal financial information
- Credit card or purchase card account numbers
- Passport numbers
- Potentially sensitive employment information, e.g., personnel ratings, disciplinary actions, and result of background investigations
- Criminal history
- Any information that may stigmatize or adversely affect an individual.

- Transcripts or forms of grades

This list is not exhaustive, and other data may be sensitive depending on specific circumstances.

Social Security Numbers (SSNs), including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual. If it is determined that such transmission is required, then secure methods must be employed.

What PII is non-sensitive?

The following additional types of PII may be transmitted electronically without protection because they are not considered sufficiently sensitive to require protection.

- Work, home and cell phone numbers
- Work and home addresses
- Work and personal e-mail addresses
- Resumes that do not include an SSN or where the SSN is redacted
- General background information about individuals found in resumes and biographies
- Position descriptions and performance plans without ratings

The determination that certain PII is non-sensitive does not mean that it is publicly releasable. The determination to publicly release any information can only be made by the official authorized to make such determinations. The electronic transmission of non-sensitive PII is equivalent to transmitting the same information by the U.S. mail, a private delivery service, courier, facsimile, or voice. Although each of these methods has vulnerabilities, the transmitted information can only be compromised as a result of theft, fraud, or other illegal activity.

May an individual employee electronically transmit PII that applies solely to the employee?

Other than the non-sensitive information identified above, individual employees, including contract employees, should not electronically transmit personal information solely about themselves unless it is encrypted or handled by a secure method. This is to ensure that the personal information is protected from possible breach and identity theft.

What does electronic transmission of PII include?

Examples of electronic transmission of PII, include, but are not limited to:

- E-mail, text, and instant messages
- Document (s) attached to an e-mail message
- File Transfer Protocol (FTP)
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- General Web Services
- File Sharing Services
- Electronic Data Interchange (EDI)

Who should employees contact if they have questions about which PII may be transmitted electronically?

If there is any question concerning the sensitive or non-sensitive nature of the PII, they should contact their supervisor who should consult BridgeValley Office of Information Technology if doubts remain.

How should operating units transmit sensitive PII?

There are several methods operating units can use to transmit sensitive PII. These include:

- Installing encryption software on a select number of desktops and designating those computers for the transmission of sensitive PII. The encryption methodology that is installed must conform to the standard for cryptographic-based security systems in Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules.
- Using encryption software to encrypt the sensitive PII before sending it electronically, e.g., as an e-mail attachment. The password key should be forwarded to the recipient in a separate e-mail from the attached file.
- Using an application designed to protect the transmission of sensitive PII, e.g., Web-based applications that use TLS1.0, secure file share, or secure file transfer applications such as Secure Shell File Transport Protocol (SFTP).
- Sending documents with sensitive PII by facsimile is permissible if the sender alerts the designated recipient that sensitive PII is being sent. The recipient must then verify by phone or e-mail that the information has been received.