Eastwick College and the Hohokus School-
Office of Information Technology
Eastwick College GBLA policy

Purpose

The purpose of this Information Security Plan ("ISP") is to describe how Eastwick Education ("Eastwick Education," "we," or "our") complies with the Gramm-Leach-Bliley Act Safeguards Rule ("GLBA") and develops, implements, and maintains appropriate administrative, technical, and physical safeguards to protect the confidentiality of Personal Information that we access, collect, distribute, process, protect, store, use, transmit, dispose, or otherwise handle.

The objectives of this ISP are to: ensure the security and confidentiality of Personal Information; protect against any anticipated threats or hazards to the security or integrity of Personal Information; and protect against unauthorized access to or use of Personal Information that could result in substantial harm or inconvenience to any individual.

We take seriously our responsibility to protect confidential information and to comply with applicable federal and state privacy and data security laws and regulations. To that end, we have implemented several policies, procedures, plans, and documents that make up our comprehensive information security program ("CISP"). Where appropriate, we reference or incorporate other policies and procedures.

Scope

This ISP applies to all Eastwick Education employees, whether full-time or part-time, including faculty, administrative staff, contract or temporary workers, consultants, interns, and student employees. This ISP also applies to certain contracted third-party vendors. This ISP applies to any Personal Information, whether in paper, electronic, or other form, that is accessed, collected, distributed, processed, protected, stored, used, transmitted, disposed, or otherwise handled by or on behalf of Eastwick Education or our affiliates. This ISP is not intended to supersede any existing Eastwick Education policy that provides more specific requirements for safeguarding certain types of data, including the definition of directory information under the Family Educational Rights and Privacy Act (FERPA).

Policy

1. Definition of personal information

"Personal Information" includes nonpublic personally identifiable financial information and other personally identifiable information.

"Nonpublic Personally Identifiable Financial Information" means any information that is not publicly available and:

An individual provides to obtain a financial product or service from Eastwick Education;
About an individual resulting from a transaction with Eastwick Education involving a financial product or service; or
Eastwick Education otherwise obtains information about an individual in connection with providing a financial product or service.

Examples of nonpublic personally identifiable financial information include (but are not limited to):

Information an individual provides to Eastwick Education on an application to obtain a student loan, credit card, or other financial product of service;
Account balance information, payment history, loan or deposit balances, debts, overdraft history, and credit or debit card purchase information;
The fact that an individual has obtained federal student aid or financial product or service from Eastwick Education;
Any information an individual provides to Eastwick Education or that Eastwick Education otherwise obtains in connection with collecting on, or servicing, a credit account;
Information from a consumer report; and
Any list, description, or other group that is derived using any nonpublic personally identifiable financial information (as described in 1-6 above) that is not publicly available.

"Personally identifiable information" generally means information that can be used to distinguish or trace an individual's identity and any other information that is linked to an individual.

Examples of Personally Identifiable Information include (but are not limited to):

First name and last name or first initial and last name

Maiden name

- Alias
- Name of student's parents or other family members
- Mother's maiden name
- Address
- Telephone number
- Fax number
- Email address
- Social media address
- Social security number
- Driver's license number, state-issued identification card number
- Federal or state government issued identification card or tribal identification card
- Passport number
- Date of birth
- Place of birth
- Financial account number
- Bank account number
- Credit or debit card number

- Password, PIN, or other access code or security code that would permit access to the person's financial account
- Tax return information, including taxpayer identification number
- Medical (mental or physical) history information
- Medical (mental or physical) condition information
- Medical (mental or physical) treatment or diagnosis information
- Health account numbers
- Health account payment information
- Health insurance information, subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history
- Medical records or medical records numbers
- Other insurance account number
- License plate number
- Device identifiers and serial numbers
- Fingerprints
- Digital signature
- Handwriting
- Biometric data - retina or iris scan, voice, facial geometry
- DNA profile
- Educational information, including performance evaluations
- Certain information Eastwick Education collects through an Internet "cookie"
- Any unique identifying number, characteristic, or code, including electronic identification number or routing code

"Personal Information" does not include:

Publicly available information, which means information that Eastwick Education has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law;
Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any Personal Information that is not publicly available; or
Information that does not identify an individual, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

2. Risk assessment

Eastwick Education recognizes that there are both internal and external risks to the security, confidentiality, and integrity of Personal Information that could result in unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information.

Eastwick Education has conducted a risk assessment of reasonably foreseeable internal and external risks to Personal Information in the following areas of operation:

> Internal Risks: Employee training and management, especially as it relates to access to and use of student records, including financial aid information;
> Operational Risks: Information systems, including network and software design, information processing, storage, transmission, and disposal; and
> External Risks: Security breaches, attacks, intrusions, and other system failures, especially as it relates to detecting, preventing, and responding to attacks or other system failures.

Based on the risks identified in the risk assessment, Eastwick Education has assessed the sufficiency of existing safeguards and has designed and implemented the following information safeguards to minimize or control identified risks. Eastwick Education will regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

Eastwick Education recognizes that risks change and new risks are created periodically. Eastwick Education will, at least annually, conduct a risk assessment and evaluate and adjust our information security program in light of the results of the testing and monitoring; any material changes to our operations or business arrangements; or any other circumstances that we know or have reason to know may have a material impact on our information security program.

3. Chief information security officer

Eastwick Education has designated Mr. Joseph Neyman as the Director of Technology to coordinate our information security program. The Director of Technology may designate other Eastwick Education representatives to oversee the program as necessary

Any questions or concerns regarding this ISP or Eastwick Education information security should be addressed to the Director of Technology at:

Joseph Neyman
Corporate Director of Information Technology
Eastwick College
10 South Franklin Turnpike
Ramsey, NJ 07446
Phone: 201.327.8877
Email: jneyman@eastwick.edu

The Director of Technology and the Eastwick college - office of technology will be responsible for implementing, supervising, and maintaining the ISP. These responsibilities include:

- Conducting ongoing training of Eastwick Education employees regarding their responsibilities and duties under the ISP;
- Regularly conducting a risk assessment of reasonably foreseeable internal and external risks to Personal Information in the three areas of operation identified above and assessing the sufficiency of existing safeguards to control identified risks;
- Regularly testing and monitoring the effectiveness of the safeguards' key controls, systems, and procedures;
- Regularly evaluating and adjusting the information security program in light of the results of tests and monitoring; any material changes to operations or business arrangements; or any other circumstances that may have a material impact on the information security program; and
- Evaluating the ability of Eastwick Education's third party service providers to implement and maintain appropriate safeguards and contractually require third party service providers to implement and maintain appropriate safeguards.

4. Internal risk safeguards

- Eastwick Education only collects Personal Information that is necessary to accomplish our legitimate business transactions or to comply with applicable laws and regulations.
- Access to Personal Information is restricted to only those employees or authorized third parties that require access in the course of their duties, based on their job description. Employees or third parties may only access Personal Information if they have a legitimate need to access such information.
- Personal Information shall only be used for authorized business purposes.
- Eastwick Education will check employee references and conduct a background check before hiring employees who will have access to Personal Information.

- **A copy of this ISP will be distributed to each current employee and each new employee on the first date of employment**. Eastwick Education will require each employee to acknowledge in writing that the employee received a copy of this document and will abide by Eastwick Education's confidentiality and security standards for handling Personal Information.
- All employees will receive initial and ongoing training regarding the ISP and the steps they need to take to protect the security, confidentiality, and integrity of Personal Information.
- The Director of Technology will provide supplemental training, education, and alerts to update employees on new security issues and threats, as applicable.
- Eastwick Education will regularly remind employees of the company policy, and the legal requirement, to keep Personal Information secure and confidential. For example, Eastwick Education will post reminders about employees' responsibility in the rooms and other locations where Personal Information is stored.
- Employees are required to immediately report suspicious activities to the Director of Technology or unauthorized use of Personal Information to the Director of Technology, including any lost or misplaced device such as a cellphone or laptop which may contain Personal Information, regardless of data encryption.
- Employees are encouraged to advise the Director of Technology of any suspicious incident, activity or operation which appears to pose a risk to the security of Personal Information. If an employee suspects the Director of Technology is involved with such risk, the employee is encouraged to inform Eastwick Education's Executive Vice President of Operations.
- Employees who violate this ISP will be subject to disciplinary action, even if no Personal Information was compromised.
- Employees will be required to use "strong" passwords (consistent with acceptable security standards) that must be changed on a regular basis. Employee computers will also have password-activated screensaver to lock employee computers after a period of inactivity. Employees will receive training on how to securely protect their passwords. Passwords must be changed every 90 days. Employees who do not change their passwords on a regular basis will be denied access to Personal Information.
- Employees are not permitted to store Personal Information at home or on their personal computers, personal laptops or personal mobile devices (e.g. USBs, flash drives, smart phones, external hard drives).
- Employees are not permitted to transport Personal Information electronically on portable storage devices (e.g. USBs, flash drives, and external hard drives) unless the transported data is encrypted.
- Employees are not permitted to access Personal Information at home or on their personal computers except when utilizing Eastwick Education's VPN software.
- Employees' personal mobile devices, tablets, and smart phones with Eastwick Education email must have an ActiveSync policy that enables encryption on the device.
- Personal Information must not be stored on cloud-based storage solutions that are unsupported by Eastwick Education.

- Employees must lock rooms or file cabinets where records containing Personal Information are kept.
- Employees must secure paper files containing Personal Information in their work area when they are not present.
- Employees must ensure Personal Information is encrypted when it is transmitted electronically via public networks.
- Laptops, cellphones, and other devices must be stored in a secure place when not in use or personally attended.
- Upon separation of an employment relationship with Eastwick Education, the separated individual's electronic and physical access to documents, systems, or networks containing Personal Information must be immediately terminated. Separated employees must return to Eastwick Education all records containing Personal Information, in any form, in their possession at the time of separation. All equipment related to technology owned by Eastwick College shall be surrendered at the time of separation.

5. Operational risk safeguards

- Eastwick Education will work to develop an inventory of all computers or other devices on which Personal Information is stored.
- Eastwick Education will work to develop an organization's records and systems to determine which records and systems contain Personal Information.
- Storage areas containing records with Personal Information must be protected against destruction or damage from physical hazards, such as fire or flood.
- Records containing Personal Information should only be kept in rooms or file cabinets that are locked when unattended.
- All computers and devices must restrict user access to employees who have an authorized and unique login ID assigned by the Director of Technology. User passwords must be stored in an encrypted format.
- All computers that have been inactive for fifteen (15) or more minutes will require re-log-in.
- When Personal Information is stored on a server or computer, the server or computer must only be accessible with a "strong" password (consistent with accepted security standards) and kept in a physically-secured area.
- When practicable, all visitors must be restricted from the areas where Personal Information is accessible or stored..
- Eastwick Education will maintain secure backup records and will keep archived data secure by storing it offline and in a physically secure area.
- Eastwick Education will only transmit Personal Information securely. All Personal Information will be encrypted before it is sent or transported electronically. Any Personal Information stored on portable devices must be encrypted. Sensitive financial data will only be transmitted using SSL or other secure connection.

- Personal Information shall not be removed from Eastwick Education premises in electronic or written form absent a legitimate business need and adherence to the security measures described herein.
- Where there is a legitimate need to provide records containing Personal Information outside Eastwick Education, electronic records must be password-protected and/or encrypted and paper records must be marked "confidential" and securely sealed.
- Paper documents containing Personal Information shall be disposed of either by burning, pulverizing, or shredding so that the Personal Information cannot be read or reconstructed.
- Electronic media, hardware, and other non-paper media, such as computers, disks, CDs, magnetic tapes, hard drives, laptops, cellphones, USBs, etc., shall be destroyed or erased so that Personal Information cannot be read or reconstructed.

6. External risk safeguards

- Eastwick Education will maintain up-to-date and appropriate programs and controls to prevent unauthorized access to Personal Information, including
    - Installing and using anti-virus, anti-spyware, and anti-malware software that updates automatically on any computer, device, network, or system that stores, processes, or transmits Personal Information;
    - Maintaining up-to-date firewalls and intrusion prevention;
    - Regularly ensuring that ports not actively used for business are closed; and
    - Regularly obtaining and installing security patches to resolve software vulnerabilities.
- The Director of Technology will promptly provide information and instructions to employees regarding any new security risks.
- Eastwick Education will use appropriate oversight and audit procedures to detect the improper disclosure or theft of Personal Information, including:
    - Keeping logs of activity on the network and monitoring them for signs of unauthorized access to Personal Information;
    - Using an up-to-date intrusion detection system that will alert of attacks;
    - Monitoring both in-and-out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from the system to an unknown user; and
- Eastwick Education will take steps to preserve the security, confidentiality, and integrity of Personal Information in the event of a security breach.
- Eastwick Education will periodically undergo a security audit by an outside organization.

7. Service providers

Any possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Personal Information, or a violation or attempted violation of the information safeguards described herein, must be reported immediately to the Director of Technology. The Director of Technology will document all reported or detected breaches and subsequent responsive action.

In the event of a breach of Personal Information, Eastwick Education will:

- Take immediate action to secure any Personal Information that has or may have been compromised;
- Preserve and review files or programs that may indicate how the breach occurred; and
- If appropriate, retain professionals to assess the breach.

Eastwick Education will follow federal and state laws and regulations concerning breach notification.

In the event of a security breach, Eastwick Education will review and implement appropriate safeguards to mitigate the reoccurrence of such a breach.

- HIPAA Privacy Policy
- Website Privacy Policy
- FERPA Policy
- Remote Access Policy
- Employee Confidentiality Policy