Information Security and Privacy Program

Policy Statement

Information security and privacy are of utmost importance to Phillips Exeter Academy. It is the responsibility of every individual who has access to the Academy's information and data assets to maintain and safeguard them from threats that could result in identity theft, fraud, business disruption, or damage to the school's reputation. Information obtained or created during the course of Academy business is the property of the Academy and the Academy expects that this information will be used for Academy purposes only and will be disclosed only to those with a need to know such information.

Purpose

The Information Security and Privacy Policy (the policy) provides guidelines and practices to ensure appropriate use of the Academy's information and data assets. The intent of the policy is to ensure the integrity and appropriate availability of data, while protecting against unauthorized access to or use of confidential data to an extent that is reasonable and practical, and to comply with the Academy's obligations under all applicable local, state, and federal regulations and contracts. Confidential data can be contained in many forms including paper, electronic and verbal and includes personal, strategic, financial, academic, health and legal data.

Scope

This policy applies to all users of Phillips Exeter Academy's information and data assets. Employees, emeriti, students, parents, alumni/ae, volunteers, third party contractors and any others who may have access to the Academy's data are responsible for being familiar with and adhering to this policy.

Authorized Use

- An authorized user is any person who has been granted authority by the Academy to access its computing systems or data. Unauthorized use is strictly prohibited.
- By accessing the Academy's data using Academy-owned or personally-owned equipment, or through non-electronic means, you have consented to the Academy's exercise of its authority and rights as set out in this policy.
- Authorization to access confidential data is based on the role and responsibilities of an individual user. If a user's role and/or responsibilities change, authorization to access confidential data will change as appropriate.

Responsible Use

- Users who have access to confidential information are required to:
  - log out of or lock your device when you walk away from your desk/device
  - use a security passcode on all devices
  - create strong passwords
  - not share your username or password with anyone
  - not store confidential data on public computers, e.g. Academy labs, classrooms or Library, hotel, airport
  - have updated anti-virus software on their computers
- Users should use caution when opening email attachments or other internet files which may contain malicious software.
- Individual users who have access to sensitive data are solely responsible for how they are used. Users must take care to prevent unauthorized access to confidential data and are prohibited from acting in ways that are unethical, illegal or invade the privacy of others.
- In an event or circumstance which is not clearly defined by this policy, users will take appropriate responsibility for the protection of confidential information, will respect the legitimate interests of others, and will strive to make decisions in the best interest of the Academy.

Data Classification

Confidential Data

The Academy relies upon the integrity of its data assets to effectively operate the school. Data that, if lost, stolen, altered or disclosed without authorization, could result in identity theft, breach of state laws, federal laws or legally binding agreements are considered **confidential**. Inappropriate use of confidential data could have a serious negative affect upon the Academy, its employees and students. Examples of confidential data include student records, social security numbers, credit card numbers, dates of birth, financial account numbers, driver's license numbers, passport/visa numbers, health insurance policy numbers, salary information and donor giving information. This data should be treated with the highest levels of security controls.

Public Data

Data is classified as **public** if there is little to no adverse impact from unauthorized disclosure or use, alteration or loss of that data or if the data is available through other public means. Little or no controls are needed to protect confidentiality and accessibility, though some level of control is required to prevent modification or destruction of public data.

Determining Classification

Data will be reviewed and categories will classified by the CFO and Director of IT. The definition of data classifications above and the characteristics noted in the table below will help determine the appropriate classification.

Characteristic	**Data Classification**	
	Confidential	**Public**
Potential negative impact or risk to the Academy, its reputation and its constituents if data is misused	Yes	No
Misuse could result in ID theft	Yes	No
Laws govern access and controls	Yes	No
Binding agreements state required controls	Yes	No
Fits pre-defined Confidential categories	Yes	No
Publicly Available in other forums (Newspapers, Websites, via Freedom of Information Act)	No	Yes

Confidential Categories

Phillips Exeter Academy has determined various categories of data that should be considered confidential. Upon review of specific data, any that fit the following categories should be treated as confidential. Permission to access this data must be provided by the Director of the noted department or the position noted as the Owner.

Category	Definitions	Examples	Owner
Authentication Verifiers	Data that provides authorized access to any Academy computing resources.	User name and Password	IT
Personally Identifiable Information (PII)	Data that can be used to assume another's identity. Restricted by state privacy laws.	Social Security Number Date of Birth Driver's license number State issued identification number Health insurance information Passport/Visa number	HR – Employees DoS – Students, Parents Admissions – Prospective students/families IA – alumni, past parents Summer School – SS students, families, alumni
Protected Health Information (PHI)	Any health information or records that can be personally identified.	Diagnosis/conditions – physical or mental Treatment information Payment information The above data combined with data that personally identifies an individual, including but not limited to: PII (see above) Name Address Telephone number	HR – Staff DoF – Faculty Medical Director - Students
Payment Card Information	Payment Card account information as defined by the Payment Card Industry Data Security Standard (PCI DSS)	Primary Account Number Cardholder Name Service Code Expiration Date Service Code CAV2, CVC2, CVV2, CID PIN Contents of magnetic strip	CFO
Financial Information	Academy financial data or financial data that can be personally identified. Restricted by regulations.	Financial account numbers Loan or Grant Information Tax return information Salary data	CFO – Academy data HR - Employees Admissions – Applicants
Personally Identifiable Education Records	Individual student record data	Transcript data, combined with data that identifies the individual: PII (see above) Name (student or parent) Student ID number	DoS CCO
Legal Data	Any data that is legal in nature or subject to attorney-client privilege	Materials subject to litigation hold Severance agreements Negotiation documents Contracts	CFO

Data Protection Standards for Confidential Data

Data Protection Standards provide users with the guidance to protect the Academy's confidential data. All users of Academy data are expected to familiarize themselves with and follow these standards.

Data Protection Standards

Media/Method	Data Protection
Academy-owned and Personally-owned Electronic Storage: - Servers - Laptops - Removable storage - Mobile devices - Remote/cloud storage	Devices must require authentication (id & password). Documents and files containing legal data must be marked "Privileged and Confidential". Documents and files containing other confidential data should be marked "Confidential". Documents and files containing confidential data must not be stored in personal cloud accounts (e.g. Dropbox). If data needs to be shared, it should be done through Academy owned means (e.g. OneDrive for business, network folders).
Physical Storage: - Paper - Microfilm	Documents and files containing legal data must be marked "Privileged and Confidential". Documents and files containing other confidential data should be marked "Confidential". Documents and files should be stored in a controlled environment and should only be provided to those with permission. Official documents and files (e.g. student files) should be maintained and disposed of according to data retention policies. Personal/individual copies must be safeguarded, and shredded after use.
E-Mail	If documents or files containing confidential data are emailed, they must be password protected. Password must be sent to recipient in a separate email. Disclaimer must be appended to end of emails that contain confidential data: *"Unauthorized disclosure of any proprietary or confidential information in this email is prohibited. If you are not the intended recipient, please notify the sender and delete this email immediately."*
Fax Transmissions	Transmissions that contain confidential data must include the disclaimer: *"Unauthorized disclosure of any proprietary or confidential information in this fax is prohibited. If you are not the intended recipient, please notify the sender and destroy this fax immediately."* Material should be marked "Confidential".
Other Electronic Transmissions	Must use secure protocols (e.g. SFTP)

Electronic Display (e.g. PowerPoint, demos)	Displayed material must be marked “Confidential”.

Data Breach Response

Confidential data that is lost, stolen or misused constitute a data breach. Data breaches will be investigated by the CFO and the Director of IT. Depending upon the nature of the issue, other participants may be included in the investigation.

Based upon the type and nature of the incident, steps taken may include:

- Analyzing and identifying the cause of the incident
- Containing damages
- Planning and implementing corrective actions to prevent recurrence
- Communicating with those affected by or involved in the recovery from the incident
- Reporting actions and events to the appropriate authorities

Enforcement and Sanctions

All members of the community are expected to assist in the enforcement of this policy. Violations of this policy may result in a variety of disciplinary actions which may include the loss of computer or network access privileges, lawsuit and/or dismissal for employees, requirement to withdraw for students or termination of vendors or volunteers.

Any suspected violation of this policy should be reported immediately to the Director of Information Technology or the CFO.

Policy Maintenance

Administration of the policy resides with the Chief Financial Officer (CFO) and Director of Information Technology (IT).

Last update: **08.26.2015**

Approved: **09.22.2015**