Media and Privacy Policies

INFORMATION SECURITY AND PRIVACY PROTECTION POLICY

Information security and privacy are of utmost importance to Fairview International Academy ("the 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 and national 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 Fairfield International Academy's information and data assets. Employees, 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 (libraries, hotels, airports, etc.)
have updated anti-virus software on your computers
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, financial 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 be classified by the Head Principal. The definition of data classifications above and the characteristics noted in the table below will help determine the appropriate classification.

Characteristic Data Classification

How to check for Confidential Public, potential negative impact or risk to the Academy, its reputation and its constituents if data is misused:

1. Misuse could result in ID theft Yes/No?
2. Laws govern access and controls Yes/No?
3. Binding agreements or state required controls Yes/No?
4. Fits pre-defined Confidential categories Yes/No?
5. Publicly Available in other forums (Newspapers, Websites, via Freedom of Information Act) Yes/No?

Confidential Categories

Fairfield International Academy has determined various categories of data that should be considered confidential. Upon review of specific data, any that fit the following categories (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, financial information and donor-giving information) should be treated as confidential. Permission to access this confidential data must be provided by the Head Principal or the person noted as the Owner.
Category Definitions Examples Owner
Academy-owned and Personally-owned Electronic Storage:

- Servers
- Laptops
- Removable storage
- Mobile devices
- Remote/cloud storage

Devices 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 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. Passwords must be sent to the recipient in a separate email.
Disclaimer must be appended to the 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."

Data Breach Response
Confidential data that is lost, stolen or misused constitute a data breach. Data breaches will be investigated by the Head Principal. 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, requirement to withdraw for students or lawsuit and/or

dismissal for employees, vendors or volunteers. Any suspected violation of this policy should be reported immediately to the Head Principal.

Policy Maintenance
Administration of the policy resides with the Head Principal.

Last update: October 2020