Computer IT and Information Security Policy

Each member of the Elite Academy community must comply with the full text of all Elite Academy policies in this document to access our computer, technology, and network resources.

Failure to follow this policy may result in disciplinary action, including termination.

Equipment and School Generated Data

Ownership

Elite Academy retains the rights and ownership of all data generated by the school systems. Examples including but not limited to: the digital logs of clocking in/out, assignments turned in to educators, and student and employee information generated and entered on school equipment, and software services.

Unless otherwise marked, data/information/curriculum materials such as documents, images, files, disclosures, and signage are owned by Elite Academy.

Protect Information and Electronic Resources

Safeguard Sensitive Information(Sensitive Data)

It is expected that students take steps to safeguard access to their personal information and data. This can be done with strong password combinations. Students should recognize that sending personal information via email may disclose their information to 3rd parties and should avoid email as a secure delivery mechanism.

Additional Security Measures

Security protections are highly recommended for all student devices connected to the network, and the school is not responsible for any lost data, ransomware, malware, or virus infection of the student's computer.

Elite Academy recommends the following:

- Regularly install software updates
- Ensure antivirus and/or anti-malware is running
- Use a host-based firewall
- Ensure adequate physical security (e.g. Login account w/ adequate password)
- Where technically supported, enable device level encryption in case your device is lost or stolen.

Reporting and Response to Security Incidents or Suspicious Activity

If you suspect your account has been compromised or hacked, report security incidents or suspicions to your Campus Director, who will refer you to the Elite Academy IT department.

Privacy of Electronic Communications

Routine Security Monitoring

Elite Academy may use 3rd parties to scan and analyze our networks for vulnerabilities and ensure the integrity and reliability of systems. The scope is typically limited to the use of techniques that include routine monitoring of electronic communications, and port scanning (e.g., scanning, bandwidth monitoring). By connecting your devices to our networks, you consent to allowing the scan and monitoring of your devices.

Keep Personal Information on Personal Devices

Personal use of electronic resources must be done on personal devices. For example, do not check your personal email or social media account on our shared student computers. This is to ensure both your information and any client information is protected.

3rd Party Information Sharing

Elite Academy works with third-party servicers to carry out business related functions and comply with other federal and state government requirements and programs. In the course of this work your student information may be shared in order to carry out the function or to properly satisfy the requirements.

Use of Text Message

Students and employees consent to receive messages (e.g. text messages, etc.) from Elite Academy. Information will not be shared or sold to third parties. Message frequency may vary, and standard messaging and data rates apply. To opt out, text “STOP” or contact the campus director at any time.

Use Campus Technology Responsibly

Campus Computer use and network access is a privilege. Users must act **responsibly** and **professionally**, **respect** the rights of other users and treat them with **civility**, respect the integrity of the systems, data, and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Use Best Practices for Protecting Privacy and Online Security

Choose Strong Passwords

Our systems will help enforce a certain level of complexity and strength for your passwords. You must choose a unique password for your Elite Academy account. Also choose unique passwords for accounts related to work with sensitive data. The specific rules for strong passwords will vary over time, and our systems will adapt to new rules over time.

Multiple Factor Authentication

Our systems may also enforce Multiple-Factor Authentication (a.k.a Multi-Factor Authentication, or MFA). Bypassing or skipping this security set up procedure is a violation of our policy if your account has Multi-Factor Authentication enabled. When setting up MFA be sure to configure both a personal phone number and personal email, in case one of them ever changes.

Recognizing a Phishing Attack

“Phishing” attacks are increasingly common, and schools and administrators are susceptible to targeted phishing schemes to mislead users to click and provide their personal information or credentials to an unauthorized party.

- Never send passwords, account info, or other private information in an email.
- Avoid clicking links in emails, especially from parties you don’t know.
- Be wary of any unexpected email attachments or links, even from people you know.