UNIVERSITY VIEW ACADEMY ACCEPTABLE USE POLICY

Revised Effective Date: July 26, 2022

This section defines the boundaries for the "acceptable use" of the employer's electronic resources, including software, hardware devices, and network systems. By using Foundation for Louisiana Students d/b/a University View Academy's ("UVA" or the "company") hardware, software, and network systems, you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable company policies, as well as city, state, and federal laws and regulations. The network and Internet user shall be held responsible for his or her actions and activities. Responsibilities include efficient, ethical and legal utilization of network resources.

SOFTWARE

All software acquired for or on behalf of the employer or developed by employees or contract personnel on behalf of the employer is company property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

Under no circumstances should any user install or download any software onto an employer-owned device without specific permission from the IT Department. This applies to unauthorized third party browser extensions that could cause potential security breaches to company information and data. If an unauthorized software is accidentally downloaded, the employee is responsible for immediately notifying the IT department.

All approved software downloaded from non-UVA sources must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine. All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

PURCHASING

All purchasing of company software(to include internet programs) and hardware will be centralized with the technology department to ensure that all applications conform to company software standards and are purchased at the best possible price. All requests for software must be submitted to the department head for approval. If approved, the request must then be sent to the technology department, which will then determine and purchase the standard software that best accommodates the desired request.

Free third party applications or software must still adhere to company software standards. Employees should reach out to the IT department if they are unsure if the privacy standards adhere to company expectations and policies prior to downloading or using.

LICENSING

UVA is responsible for enforcing all applicable licenses, notices, contracts, and agreements for software that is used on company computers. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of federal and state law. We must strictly enforce license compliance as any violation by an employee may still cause UVA to be liable for the consequences of such violation.

HARDWARE

All hardware devices acquired for or on behalf of the employer or developed by employees or contract personnel on behalf of the employer is and shall be deemed the employer's property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

ELECTRONIC COMMUNICATIONS, TELEPHONE COMMUNICATIONS AND ACCESS CONTROL SECURITY POLICY

As a productivity enhancement tool, the employer encourages the business use of electronic communications (including phone, voicemail, e-mail, webmail, message boards, instant message and fax). All messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of the employer, and are not the property of users of the electronic communications services.

Business phones may be monitored or recorded to ensure quality and in some departments, business phones may not be used for personal calls, depending on the nature of the work. In some departments, personal cell phones may only be used in break areas during employees' scheduled breaks and lunches.

AUTHORIZED USAGE

The employer's electronic communications and telecommunications systems generally must be used only for business activities. Incidental personal use is permissible so long as:

1. It does not preempt any business activity.
2. It does not consume more than a trivial amount of time and/or resources.
3. It does not interfere with staff productivity.

Users are prohibited from using company electronic communications and telecommunications systems for charitable endeavors, private business activities, or amusement/entertainment purposes unless approved by their supervisor in writing. Employees are reminded that the use of company resources, including electronic communications and telecommunications systems, should never create either the appearance or the reality of inappropriate use.

Some departments may explicitly prohibit personal internet usage on the company's network. This will be outlined in a department specific policy.

Use of the network for any illegal activities shall also be prohibited. Illegal activities include (a) tampering with computer hardware or software, (b) unauthorized entry into computers and files (hacking), (c) knowledgeable vandalism or destruction of equipment, and (d) deletion of computer files. Such activity is considered a crime under state and federal law. The University View Academy Board shall not condone the use of the Internet for any illegal or inappropriate activities and shall not be responsible for any such use by staff or students.

COMMUNICATION USING UVA ISSUED TECHNOLOGY

Employees are prohibited from using UVA Technology for any purpose not related to their job function at UVA.

Information related to a specific student should never be posted to external sites. Internal postings by employees, teachers or other individuals who are not the learning coaches for currently enrolled students will be limited to comments relating to the program or other school-related activities. Further, such postings should be limited to those necessary to answer posted questions, to assist with identified problems or to gather parent input on proposed program changes or other school topics.

Employees must not place company material on any publicly accessible site that supports anonymous viewing or distribution.

Employees shall not post any e-mail or other messages or materials on company networks or the Internet that are indecent, vulgar, lewd, slanderous, abusive, threatening, sexually harassing, or terrorizing.

EMAIL/WEBMAIL

Misuse of email can pose many legal, privacy and security risks, thus it's important for employees to understand the appropriate use of electronic communications. For the purposes of this section, webmail is defined as any communication sent from any UVA provided account that has communication capabilities.

1. UVA email account should not be used for personal communications.
2. The University View Academy email/webmail systems shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any University View employee should report the matter to their supervisor immediately.
3. Users shall not use technology resources to further other acts that are criminal or violate the schools code of conduct or rules.
4. Users shall not disclose, use, or disseminate personal information regarding minors.

5. Users shall not use the e-mail system for commercial, political, personal activities, or religious purposes.
6. Users are prohibited from automatically forwarding University View Academy email/webmail to a third party email system. Individual messages which are forwarded by the user must not contain University View Academy confidential information
7. Users are prohibited from using third-party email (personal or consumer) systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct University View Academy business, to create or memorialize any binding transactions, or to store or retain email on behalf of University View Academy. Such communications and transactions should be conducted through proper channels using University View Academy-approved documentation.
8. Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Sensitive information must not be forwarded to any external party without the prior approval of your department head. Blanket forwarding of messages to parties outside the organization is prohibited unless the prior permission of the Superintendent has been obtained.
8. University View Academy employees shall have no expectation of privacy in anything they store, send or receive on the company's email system or a company issued device.
9. Any emails that are sent using the company email/webmail systems, whether or not the users are employees, are the property of the employer and may be viewed by members of management or others with administrative rights to the system. Furthermore, the technology department is instructed to forward to management any emails that violate our Internet usage policy or represent activities that could be detrimental to the company's operations.
10. University View Academy may monitor messages without prior notice. University View Academy is not obliged to monitor email messages. Employees should be aware that electronic and telephone communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others may require access to electronic and telephone communications in accordance with this policy.
11. It is our policy not to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that we may examine the content of electronic communications.
12. It may be necessary for technology department staff to review the content of an individual employee's communications during the course of problem resolution. Technology department staff may not review the content of an individual's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels
11. Employees are expected to communicate in a professional manner consistent with state laws and Board policies governing the behavior of school employees and with federal laws governing copyright. Electronic mail and telecommunications are not to be utilized for unauthorized disclosure, use and dissemination of personal identification or confidential information regarding any student or employee.

GENERAL ELECTRONIC COMMUNICATIONS PROVISIONS & DEFAULT PRIVILEGES

User privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "least privilege." With the exception of emergencies and regular system maintenance notices, broadcast facilities (including the "All-Employees" distribution list) must be used only after the permission of your department head has been obtained.

SECURITY

Teachers and personnel shall be responsible for the security of those computers in terms of both hardware and software. Computers must be secured such that others acting without the consent or supervision of a teacher or administrator cannot enter the system or the Internet from your assigned device.

All personnel will follow all security and confidentiality regulations regarding student information and records, including all electronic records (SER, SER IEP, SASI, and any other data).

No outside equipment or hardware may be plugged into the employer's network without specific permission from the technology department (including USB peripherals and Flash Drives).

USER ACCOUNTABILITY

Regardless of the circumstances, your individual user account passwords must never be shared or revealed to anyone else. This includes logging into a company resource as you allow another user to access those resources. If another user does not have access to a resource and asks you to log in for them, you should deny the request and notify the technology department immediately. If users need to share computer resident data, they should utilize public directories on local area network servers. Users should also refrain from sending attachments to internal users for review and comment if the resource is available in the public folder on the employer's network.

Unless tools like privacy enhanced mail (PEM) are used, it is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with company information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal information.

To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities), and enable two-factor authentication on all UVA accounts where it is available. The employer's password policy requires users to choose a password that is at least 8 characters long and a combination of letters, numbers and/or symbols. You may be

required to change your password every 90 days, and you are not permitted to re-use your previous 5 passwords.

The company shall incorporate the use of computer-related technology or the use of Internet service provider technology designed to block access or exposure to any harmful materials or information, such as sites that contain obscene, pornographic, pervasively vulgar, excessively violent, or sexually harassing information or material. Sites which contain information on the manufacturing of bombs or other incendiary devices shall also be prohibited. However, the company shall not prohibit authorized employees or students from having unfiltered or unrestricted access to Internet or online services, including online services of newspapers with daily circulation of at least 1,000, for legitimate scientific or educational purposes approved by the company.

STATISTICAL DATA

Consistent with generally accepted business practice, we collect statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, the technology department staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

PURGING ELECTRONIC MESSAGES

Sent and received emails should also regularly be purged from your personal electronic message storage areas. Deleting unneeded messages is also necessary to keep our email servers from being overloaded. Each email account has a storage limitation that will notify you when the maximum space in your account has been reached. At that point, you are required to archive or delete your non-essential email to make more room in your mailbox. As a Louisiana public charter school, we are subject to public records requests from members of the press or others. We may also be subject to litigation "holds" or other similar requests which may impact this policy for purging electronic messages. Once such a request has been made, it could be a criminal offense to delete content that could be covered by the request, even if the person who deleted the content genuinely believes that the deleted content was not relevant. We will notify personnel if there has been a public records request, litigation "hold" or other similar request, and we will provide instructions for preserving emails and other documents.

INTERNET SECURITY & USAGE POLICY

All information traversing company computer networks that has not been specifically identified as the property of other parties will be treated as though it is a company asset. It is our policy to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is our policy to protect information belonging to third parties that has been entrusted to us in confidence as well as in accordance with applicable non-disclosure agreements, contracts and industry standards.

Exceptions

Any exception to the policy must be approved by appropriate parties as identified by the Superintendent and/or Board of Directors in advance.

Non-Compliance

The company does not condone any illegal or inappropriate activities and shall not be responsible for such use by staff. The company does not guarantee the right to use the Internet and reserves the right to suspend or terminate the privilege of any individual at its sole discretion without notice, cause, or reason. Failure to adhere to these policies may result in the loss of computer privileges, access to the Internet and electronic mail accounts, and may result in further disciplinary action, up to and including termination of employment.

No personal or student information which is protected by the *Family Education Rights and Privacy Act* (FERPA) shall be disseminated on or through the company's technology systems and networks, including but not limited to the Internet.

The above acceptable use practices are not all-inclusive but are only representative and illustrative. A user who commits an act of misconduct, which is not listed, may also be subject to disciplinary action or termination. Furthermore, any activity that may be in violation of local, state, or federal laws shall be reported to the appropriate law enforcement agency.

Sign to indicate that you have received and agree to follow UVA's Acceptable Use Policy.

Employee Signature:_____
Employee Name: _____
Date: _____