



RISE CHARTER SCHOOL

Policy 5450: Employee Electronic Mail and On-Line Usage

Status: 2nd Reading

Original Adopted Date:

Last Reviewed Date:

Employee Electronic Mail and On-Line Services Usage

RISE Charter School contracts with the Kimberly School District for the provision and management of its technology services, including electronic communication systems, network access, and related digital resources. Therefore, RISE Charter School adopts and follows the Kimberly School District's policy governing Employee Electronic Mail and On-Line Usage to ensure consistent expectations, compliance with applicable laws, and responsible use of District/Charter-provided electronic information services and networks by all employees.

Internet access and interconnected computer systems are available to the Charter's employees. Electronic networks, including the internet, are a part of the Charter's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

Employees may, consistent with the computer use policies of the Charter and the Charter's educational goals, use approved internet sites throughout the curriculum.

The Charter email and internet systems are provided for educational purposes only. The Charter's electronic network is part of the curriculum and is not a public forum for general use.

Because of the unique nature of e-mail/Internet, and because of the Charter's desire to protect its interest with regard to its electronic records, the following rules have been established to address e-mail/Internet usage by all employees:

Uses

The use of the Charter's electronic network must be in support of the education and/or research, and in furtherance of the Charter's stated educational goals and legitimate school business purpose.

Use for other informal or personal purposes is permissible within reasonable limits provided it does not interfere with work duties and complies with Charter policy. All email and internet

records are considered Charter records and should be transmitted only to individuals who have a need to receive them and only relating to educational purposes. Employees have no expectation of privacy in any materials that are stored, transmitted, or received via the Charter's electronic network or Charter computers. The Charter reserves the right to access, monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of the computer network and internet access and any and all information transmitted or received in connection with such usage, including email and instant messages.

Unacceptable Uses of Network

The following are considered examples of unacceptable uses and constitute a violation of this policy. Additional unacceptable uses can occur other than those specifically listed or enumerated herein:

1. Uses that violate the law or encourage others to violate the law including local, State, or federal law; accessing information pertaining to the manufacture of weapons; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials;
2. Uses that cause harm to others or damage their property, person, or reputation, including but not limited to engaging in defamation; employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating; reading or sharing another person's communications or personal information; or otherwise using their access to the network or the internet;
3. Uploading a worm, virus, other harmful form of programming or vandalism; participating in hacking activities or any form of unauthorized access to other computers, networks, or other information. Employee will immediately notify the school's system administrator if they have identified a possible security problem;
4. Downloading the TikTok app or visiting the TikTok website;
5. Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying (defined as using a computer, computer system, or computer network to convey a message in any format that is intended to harm another individual);
6. Uses that jeopardize the security of access and of the computer network or other networks on the internet; uses that waste Charter resources;
7. Uses that are commercial transactions, including commercial or private advertising;

8. The promotion of election or political campaigns, issues dealing with private or charitable organizations or foundations, ballot issues, or proselytizing in a way that presents such opinions as the view of the Charter;
9. Sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, materials that depict the sexual exploitation of minors, or other inappropriate materials;
10. Sharing one's password with others or allowing them to use one's account;
11. Downloading, installing, or copying software or other files without authorization of the Executive Director or the Executive Director's designee;
12. Posting or sending messages anonymously or using a name other than one's own;
13. Attempting to access the internet using means other than the Charter network while on campus or using Charter property;
14. Sending unsolicited messages such as advertisements, chain letters, junk mail, and jokes;
15. Sending emails that are libelous, defamatory, offensive, or obscene;
16. Notifying patrons or the public of the occurrence of a school election by providing anything other than factual information associated with the election – such as location, purpose, etc. Such information shall not promote one position over another;
17. Forwarding or redistributing the private message of an email sender to third parties or giving the sender's email address to third parties without the permission of the sender; and/or
18. Downloading or disseminating copyrighted or otherwise protected works without permission or license to do so.

Software and Equipment

To ensure compliance with applicable law, provide accurate inventory information and promote systems interoperability and compatibility. Only Charter approved software will be installed by designated personnel on networks or individual machines. Appropriate licenses must be held for all software. Licenses and installation of media, physical or electronic will

be retained by the tech department. Peripheral devices (including, but not limited to, printers, scanners, and storage/data devices) must be approved and installed by designated personnel. Donated equipment and software are subject to the same policies. Service and support for personal devices will not be provided by Charter employees. All purchases of software and equipment connected to or using Charter provided network services require approval by the Tech Director.

Wireless

Wireless access is provided for Charter approved devices. Other devices, including personal employee devices, may be provided with access if resources are available. The access to personal devices will be limited to resources available to the public via the Internet. Employees are prohibited from establishing network services of any kind or interfering with Charter services.

Outsourcing of Services

To provide more efficient service and cost effectiveness, it may be desirable to outsource various services. To ensure compatibility with existing systems, regulatory compliance, and to avoid duplication or conflicts in service, contracts for such services require the approval of the technical director and the Executive Director.

Contracts for outsourced services shall include specific language to assure the vendor will not use data for any purpose other than providing the outsourced service such as data mining for the vendor's own benefit or re-disclose it to others without appropriate authorization. The contract shall require the vendor to give us notice of any security/data breaches, and, to the extent that user notification is legally required, such notice should preferably be in advance of user notification.

Vendors shall provide tools that allow the Charter to access data in the event of the need for discovery.

The contract shall expressly make clear that all data belongs to the Charter and that the vendor acquires no rights or licenses, including without limitation of intellectual property rights or licenses, to use the data for its own purposes.

Representation of Charter

Posting of any material representing the Charter on non-Charter sites is prohibited unless approved by the Executive Director.

Records and Privacy

The Charter provides e-mail and Internet access and requires employees to use them in the performance of their duties for the Charter. All school Charter business conducted electronically will be done so utilizing Kimberly School Charter provided services.

Access to non-Charter services for the purpose of collaboration related to Charter assigned duties may be approved by an immediate supervisor on a limited time, case by case basis. E-mail messages and Internet records are to be treated like shared paper files, with the

expectation that anything in them is available for review.

Charter records, including email and internet records may be subject to public records requests, disclosure to law enforcement or government officials, or to other third parties through subpoena or other processes. The Executive Director or their designee may review any and all email of any employee, at any time, with or without cause. Consequently, employees should always ensure that all information contained in email and internet messages is accurate, appropriate, and lawful. When sending student records or other confidential information by email, employees shall be aware of the security risks involved and shall take all steps directed by the Charter to reduce such risks.

The Charter shall provide directions to employees on how to send student records or other confidential information by email in a secure manner if that need arises.

When communicating with students and parents by email, employees should use their Charter email rather than a personal email account. Email and internet messages by employees may not necessarily reflect the views of the Charter. Abuse of the email or internet systems, through excessive and/or inappropriate personal use, or use in violation of the law or Charter policies, will result in disciplinary action, up to and including termination of employment.

Limited personal use shall not interfere with the educational goals or instructional objectives of the Charter. Information forwarded to non-Charter accounts shall not contain material that would constitute a breach of confidentiality or contain educational records. All email is archived for a period of at least five years.

Email may be pushed to personal devices of Charter employees. The employee shall provide password protection for the device and exercise due diligence to protect sensitive Charter information.

Charter e-mail addresses will not be linked to personal/social networking accounts and social websites.

Internet Access Conduct Agreements

Each employee will be required to sign the Procedure 5450F Employee Electronic Mail and Online Services Use Policy Acknowledgment upon the adoption of this policy or upon hiring.

Warranties/Indemnification

The Charter makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the internet provided under this policy. The Charter is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the internet. The Charter will not be responsible for any unauthorized charges or fees resulting from access to the internet, and any user is fully responsible to the Charter and

shall indemnify and hold the Charter, its Trustees, administrators, teachers, and employees harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user.

Violations

If any employee violates this policy, they may be subject to disciplinary action. The system administrator and/or the building principal or Executive Director will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations. Actions which violate local, State, or federal law may be referred to the local law enforcement agency.

Legal References	Description
531 P.2d 588 (1975)	Board of County Commissioners v. Idaho Health Fac. Auth.
IC § 18-6726	TikTok Use by State Employees on a State-Issued Device Prohibited
Idaho Executive Order	2022-06

Policy History:

Adopted on:

Revised on:

Reviewed on: