LEWISTON-PORTER CENTRAL SCHOOL DISTRICT

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

The Board will provide staff with access to various computerized information resources through the District's Computer System (DCS) consisting of software, hardware, computer networks, wireless networks/access and electronic communication systems. This may include access to electronic mail, so-called "on-line services" and the "Internet." It may also include the opportunity for staff to have independent access to the DCS from their home or other remote locations, and/or to access the DCS from their personal devices. All use of the DCS and the wireless network, including independent use off school premises and use on personal devices, shall be subject to this policy.

The Board encourages staff to make use of the DCS to explore educational topics, conduct research and contact others in the educational world. Staff members are encouraged to utilize electronic communications in their roles as employees of the District, and are encouraged to utilize electronic means to exchange communications with parents/guardians or homebound students, subject to appropriate consideration for student privacy. Such usage shall be limited to school related issues or activities. Communications over the DCS are often public in nature; therefore, general rules and standards for professional behavior and communications will apply.

The Board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. To that end, the Board directs the Superintendent their designee(s) to provide staff with training and/or notification in the proper and effective use of the DCS.

Staff use of the DCS is conditioned upon receipt of a signed acknowledgement by the staff member that he or she has reviewed and understands this policy and agrees to comply therewith, along with any other policy or regulation adopted to ensure acceptable use of the DCS. All such agreements shall be maintained by the District.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff. Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees. The Board of Education requires that all School District employees maintain a professional, ethical relationship with District students that is conducive to an effective, safe learning environment; and that staff members act as role models for students at all times, whether on or off school property and both during and outside of school hours.

Access to confidential data is a privilege afforded to District employees in the performance of their duties. Safeguarding this data is a District responsibility that the Board of Education takes very seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use mobile/personal devices to access the DCS and the information it may contain.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage.

Continued

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

District staff shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy protected by federal and state law.

Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the law and in accordance with applicable collective bargaining agreements. Legal action may be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the District.

Social Media Use by Employees

The District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach and ensure responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. Therefore, the Board of Education encourages the use of District approved social media tools and the exploration of new and emerging technologies to supplement the range of communication and educational services.

For purposes of this Policy, the definition of public social media networks or Social Networking Sites (SNS) are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the School District community which do not fall within the District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, Vine, Instagram, SnapChat, blog sites, etc.). The definition of District approved password-protected social media tools are those that fall within the District's electronic technology network or which the District has approved for educational use. Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access.

The use of social media (whether public or internal) can generally be defined as Official District Use, Professional/Instructional Use and Personal Use. Please note that personal use of these media during District time or on District-owned equipment is prohibited**.** In addition, employees are encouraged to maintain the highest levels of professionalism when communicating, whether using District devices or their own personal devices, in their professional capacity as educators. They have a responsibility to address inappropriate behavior or activity on these networks, including requirements for mandated reporting and compliance with all applicable District policies and regulations.

Confidentiality, Private Information and Privacy Rights

Confidential and/or private data, including but not limited to, protected student records, employee personal identifying information, and District assessment data, shall only be loaded, stored or transferred to District-owned devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and devices within the DCS, any mobile devices, including flash or key drives, and any devices that access the DCS from remote locations. Staff will not use email to transmit confidential files in order to work at home or another location. Staff will not use cloud-based storage services (such as Dropbox, GoogleDrive, SkyDrive, etc.) for confidential files.

Continued

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

Staff will not leave any devices unattended with confidential information visible. All devices are required to be locked down while the staff member steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Staff data files and electronic storage areas shall remain District property, subject to District control and inspection. The Technology Coordinator may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should **NOT** expect that information stored on the DCS will be private.

Implementation

Administrative regulations will be developed to implement the terms of this policy, addressing general parameters of acceptable staff conduct as well as prohibited activities so as to provide appropriate guidelines for employee use of the DCS.

NOTE: Refer also to Policies

#5672 - Information Security Breach and Notification
#6180 - Staff-Student Relations (Fraternization)
#6411 - Use of Email in the School District
#7243 - Student Data Breaches
#7315 - Student Use of Computerized Information Resources (Acceptable Use)
#7316 - Student Use of Personal Technology
#8271 - Internet Safety/Internet Content Filtering Policy

Adoption Date: 06/17/2024

SUBJECT: USE OF EMAIL IN THE DISTRICT

Overview

Email is a valuable tool that allows for quick and efficient communication. However, careless, unacceptable, or illegal use of email may place the District and members of its community at risk. Use of email in the District must be consistent with the District's educational goals and comply with federal and state laws and regulations, as well as all applicable District policies, regulations, procedures, collective bargaining agreements, and other related documents such as the District's *Code of Conduct*. This includes, but is not limited to, this policy and the District's policies on non-discrimination and anti-harassment, protecting the personal information of District employees and students, acceptable use, and record management.

District-related emails are most secure and best managed when District email services are used. Accordingly, the District's email services should be used for all district-related emails, including emails in which students or student issues are involved. Personal email accounts should not be used to conduct District-related business. Further, District email accounts should not be used as any individual's primary personal email address.

Scope and Application of Policy

This policy applies to all District employees and any individual assigned a District email address to conduct District-related business (authorized user).

Sending Emails with Personal, Private, and Sensitive Information

Personal, private, and sensitive information (PPSI) is any information to which unauthorized access, disclosure, modification, destruction, use, or disruption of access or use could have or cause a severe impact on critical District functions, employees, students, third parties, or other individuals or entities. For purposes of this policy, PPSI includes, but is not limited to:

a) District assessment data;

b) Protected student records;

c) Information subject to laws protecting personal information such as Family Educational Rights and Privacy Act (FERPA), Individuals with Disabilities Act (IDEA), Health Insurance Portability and Accountability Act (HIPAA);

d) Social security numbers;

e) Driver's license or non-driver identification card numbers;

f) Credit or debit card numbers;

g) Account numbers;

Continued

SUBJECT: USE OF EMAIL IN THE DISTRICT

h) Passwords; and

i) Access codes.

The failure to follow proper security protocols when emailing PPSI increases the risk that unauthorized individuals could access and misuse PPSI.

District employees and authorized users may not send or forward emails that include:

a) PPSI without building principal or supervisor authorization. Additional precautions, such as encrypting the email in a District-approved method, should be taken when sending any emails containing PPSI.

b) Lists or information about District employees without building principal or supervisor authorization.

c) Attachments with file names that may disclose PPSI. Files containing PPSI should be password protected and encrypted. File protection passwords should not be transmitted via email. District employees and authorized users will not use cloud-based storage services (such as Google Drive, Dropbox and/or OneDrive) to transmit files with PPSI without previous District approval or consulting with a building principal or supervisor. Sharing over the cloud is permitted when restricting access to authorized viewers only.

d) Comments or statements about the District that may negatively impact it.

Any questions regarding the District's protocols for sending emails with PPSI or what information may or may not be emailed should be directed to a supervisor.

Receiving Suspicious Emails

Social engineering attacks are prevalent in email. In a social engineering attack, an attacker uses human interaction (social skills) to obtain confidential or sensitive information.

Phishing attacks are a form of social engineering. Phishing attacks use fake email messages pretending to represent a legitimate person or entity to request information such as names, passwords, and account numbers. They may also deceive an individual into opening a malicious webpage or downloading a file attachment that leads to malware being installed.

Malware is malicious software that is designed to harm computer systems. Malware may be inadvertently installed after an individual opens an email attachment, downloads content from the Internet, or visits an infected website.

Continued

SUBJECT: USE OF EMAIL IN THE DISTRICT

Before responding to any emails, clicking on any hyperlinks, or opening any attachments, District employees and authorized users should review emails for indicators of suspicious activity. These indicators include, but are not limited to:

a) Attachments that were not expected or make no sense in relation to the email message;

b) When the recipient hovers the mouse over a hyperlink that is displayed in the email, the link to the address is for a different website;

c) Hyperlinks with misspellings of known websites;

d) The sender is not someone with whom the recipient ordinarily communicates;

e) The sender's email address is from a suspicious domain;

f) Emails that are unexpected, unusual, or have bad grammar or spelling errors; and

g) Emails asking the recipient to click on a link or open an attachment to avoid a negative consequence or to gain something of value.

District employees and authorized users should forward suspicious emails to the District's information technology (IT) staff.

No Expectation of Privacy

District employees and authorized users should have no expectation of privacy for any email messages they create, receive, or maintain on their District email account. The District has the right to monitor, review, and audit each District employee's and authorized user's District email account.

Accessing District Email Services on Personal Devices

In the event a District employee or authorized user loses a personal device that has been used to access the District's email service, that District employee or authorized user should notify the Districts' IT staff so that measures can be taken to secure the email account.

Personal Use

The District's email services are intended for District-related business only. Incidental or limited personal use of the District's email services is allowed so long as the use does not interfere with job performance. However, District employees and authorized users should have no expectation of privacy in this email use.

Continued

SUBJECT: USE OF EMAIL IN THE DISTRICT

The District's email services should not be used to conduct job searches, post personal information to bulletin boards, blogs, chat groups, and list services, etc. without authorization from a building principal or supervisor.

It is prohibited to use the District's email services for:

a) Illegal purposes;

b) Transmitting threatening, obscene, discriminatory, or harassing materials or messages;

c) Personal gain or profit;

d) Promoting religious or political causes; and/or

e) Sending spam, chain letters, or any other type of unauthorized widespread distribution of unsolicited mail.

Personal email accounts or services (Yahoo, Gmail, etc.) should not be accessed via the District Computer System (DCS) without authorization from a building principal or supervisor.

Confidentiality Notice

A standard confidentiality notice will automatically be added to each email as determined by the District.

Training

District employees and authorized users will receive ongoing training related to the use of email in the District. This training may cover topics such as:

a) What is expected of users, including the appropriate use of email with students, parents, and other individuals to avoid issues regarding harassment and/or charges of fraternization;

b) How to identify suspicious emails, as well as what to do after receipt of a suspicious email;

c) Emailing PPSI;

d) How to reduce risk to the District;

e) Cost of policy non-compliance;

f) Permanence of email, including how email is never truly deleted, as the data can reside in many different places and in many different forms; and

g) How users should have no expectation of privacy when using the DCS or any District email service.

Continued

SUBJECT: USE OF EMAIL IN THE DISTRICT

Notification

The District will provide annual notification of this policy and any corresponding regulations to all District employees and authorized users. The District will then require that all employees and authorized users acknowledge that they have read, understood, and will comply with the policy and regulations.

Records Management and Retention

The same laws and business records requirements apply to email as to other forms of written communication.

Email will be maintained and archived in accordance with Retention and Disposition Schedule for New York Local Government Records (LGS-1) and as outlined in any records management policies, regulations, and/or procedures.

Additionally, emails may be subject to disclosure under the Freedom of Information Law (FOIL), a court action, an audit, or as otherwise required or permitted by law or regulation.

Disciplinary Measures

Failure to comply with this policy and any corresponding regulations or procedures may subject a District employee and authorized user to discipline such as loss of email use, loss of access to the DCS, and/or other disciplinary action up to and including termination. When applicable, law enforcement agencies may be contacted.

The District's IT staff may report inappropriate use of email by a District employee or authorized user to the District employee or authorized user's building principal or supervisor who may take appropriate action which may include disciplinary measures.

NOTE: Refer also to Policies #3320 - Confidentiality of Computerized Information
#3420 - Non-Discrimination and Anti-Harassment in the District
#5670 - Records Management
#6410 - Staff Acceptable Use Policy
#8271 - Internet Safety/Internet Content Filtering

Adoption Date: 06/17/2024

LEWISTON-PORTER CENTRAL SCHOOL DISTRICT

2024 6420

Personnel

SUBJECT: EMPLOYEE PERSONNEL RECORDS AND RELEASE OF INFORMATION

Personnel Records

Administrative regulations will be developed to implement the terms of this policy to maintain a personnel file for each teacher, administrator and support staff member employed by the District.

Regulations and procedures will be developed addressing the inspection by District employees of their personnel files.

Release of Personnel Information

All steps should be taken to protect the privacy of the employees of the Board. To ensure the individual's privacy, directory or confidential information should not be shared with a third party except in the following situations:

a) When members of the Board need information from the employee's personnel record to aid them in performing their legal responsibilities in such matters as appointments, assignments, promotions, demotions, remuneration, discipline, dismissal or to aid in the development and implementation of personnel policies.

b) When the employee grants permission.

Procedures for obtaining consent for release of records to third parties shall be developed by the administration.

Release of Information Concerning Former Employees

The District shall not release information concerning the employment records, personnel file or past performance of a former employee, unless such information is required to be disclosed by law. Only the initial and final dates of employment and the position held shall be provided through a written response to a written request. The former employee may authorize the release of any additional information.

8 New York Code of Rules and Regulations
(NYCRR) Section 84
Public Officers Law Section 87

Adoption Date: 06/17/2024

LEWISTON-PORTER CENTRAL SCHOOL DISTRICT

2024 6430

Personnel

SUBJECT: EMPLOYEE ACTIVITIES

Political Activities

The Board recognizes the right of its employees, as citizens, to engage in political activities and to exercise their constitutionally-protected rights to address matters of public concern.

However, a District employee's constitutional rights to raise matters of public concern are limited when the speech or action occurs on school grounds and/or during school times. When such speech or action occurs on school grounds and/or during school time, the Board can impose reasonable restrictions on the time, place and manner of the speech or action, and can further regulate the content of such speech when it materially imperils the efficient operation of the school.

Teachers may not use their classrooms or school surroundings as a means to promote their personal political views and beliefs. However, teachers are encouraged to address issues of current events for their instructional and informational value to students, to invite public and/or political figures to visit the classroom as a community resource, and to motivate students to participate in the political process.

Solicitations by Staff

Staff members shall not be engaged in advertising or commercial solicitations on school time, except as authorized by the Superintendent/designee.

NOTE: Refer also to Policy #5560 - Use of Federal Funds for Political Expenditures

Adoption Date: 06/17/2024

SUBJECT: WHISTLEBLOWER POLICY

The Board expects officers and employees of the district to fulfill the public's trust and to conduct themselves in an honorable manner, abiding by all district policies and regulations and by all applicable state and federal laws and regulations.

However, when District officers or employees know or have reasonable cause to believe that serious instances of wrongful conduct (e.g., mismanagement of district resources, unethical behavior, violations of law or regulation, and/or abuse of authority) have occurred, they should report such wrongful conduct to the Board or one of its designated officers.

Education Law §3028-d protects District employees from retaliatory action for making a report, in good faith, to a District official, the State Comptroller's office, the Commissioner of Education or to law enforcement authorities whenever the employee has reasonable cause to suspect that a fiscal practice or action of a District employee or officer violates any local, state, federal law or rule and regulation relating to the financial practices of the District. District employees are also entitled to immunity from any civil liability that may arise from the making of such report.

Civil Service Law §75-b prohibits the dismissal or discipline of, or other adverse personnel action against, a District employee because the employee has disclosed information to a governmental body regarding (i) a violation of a law, rule, or regulation which creates a substantial and specific danger to the public health or safety, or (ii) which the employee reasonably believes to be true and reasonably believes constitutes an improper governmental action, provided, the employee has first made a good faith effort to report the information to the District and allowed the District a reasonable period of time to take appropriate action.

Reporting Responsibility

Board Policy #6110, entitled Code of Ethics for all Board Members and District Personnel (the "Code"), requires Board members and all employees of the District to observe the rules of conduct set forth in the Code in addition to prohibitions contained in any general or special law relating to ethical conduct of Board members and District employees. In addition to reporting violations pursuant to the above cited statutes, it is the responsibility of all employees and members of the Board to comply with the Code and to report violations or suspected violations in accordance with this Policy.

No Retaliation

A District employee shall not suffer harassment, retaliation or adverse employment consequences for making such a report in good faith. Any District officer or employee who retaliates against someone who has reported a violation in good faith is subject to appropriate discipline up to and including termination of employment. This Policy is intended to encourage and enable employees and others to raise serious concerns within the District prior to seeking resolution outside the District.

Continued

SUBJECT: WHISTLEBLOWER POLICY

Reporting Violations

The District shall have an open door policy for employees to share their questions, concerns, suggestions or complaints with a District officer or employee who can address them properly. In most cases, an employee's supervisor will be in the best position to address an area of concern. However, if an employee is not comfortable speaking with their supervisor or is not satisfied with the supervisor's response, the employee is encouraged to speak with the District's Assistant Superintendent for Administrative Services or any administrator who the employee is comfortable in approaching.

An administrator who receives a report of a suspected violation pursuant to this policy shall forward such report to the Superintendent without delay. In the event the report relates to actions of the Superintendent, the receiving administrator shall refer the same to the President of the Board of Education for further action.

The Superintendent (or the Board President, as the case may be) shall take immediate steps to conduct an investigation and implement appropriate corrective action if warranted. The Superintendent (or the Board President, as the case may be) shall also acknowledge the report in writing, maintain a written record of the report, insure that appropriate governmental agencies or law enforcement authorities are notified, and keep the Board informed of significant developments as and when appropriate.

Accounting and Auditing Matters

The District's Audit Committee shall address all reported concerns or complaints regarding the District's accounting practices, internal controls or auditing. The Superintendent shall notify the Audit Committee of any such complaint and shall work with the committee until the matter is resolved.

Confidentiality

The Superintendent shall make all reasonable attempts to keep the report and the identity of the employee making such report confidential, provided that doing so does not interfere with the conduct of the investigation, the rights of the person who is the subject of the report, or the implementation of corrective action.

Acting in Good Faith

Anyone who files a complaint alleging a violation or suspected violation of the Code or any statute, rule, regulation or District policy must be acting in good faith and have reasonable grounds for believing that the information disclosed is a violation of the Code, statute, rule, regulation or District policy. The making of allegations that are not ultimately substantiated and which prove to have been made maliciously or with the knowledge that they were false will be viewed as a serious disciplinary offense.

Distribution of the Policy

This policy shall be published in employee handbooks, posted on the District website and given to all employees with fiscal accounting and/or money handling responsibilities on an annual basis.

Education Law §3028-d Civil Service Law §75-b

Adoption Date: 06/17/2024

LEWISTON-PORTER CENTRAL SCHOOL DISTRICT

2024 6450

Personnel

SUBJECT: THEFT OF SERVICES OR PROPERTY

The theft of services or property from the District by an employee will result in immediate disciplinary action which can lead to dismissal or other penalty, and shall not preclude the filing of criminal or civil charges by the District.

Adoption Date: 06/17/2024