INVER GROVE HEIGHTS SCHOOLS ISD 199

EMPLOYEE ELECTRONIC TECHNOLOGIES ACCEPTABLE USE POLICY

POLICY: 424
ADOPTED: 04/27/20

I. Purpose

The purpose of this policy is to set forth policy and guidelines for employee access to the school district electronic technologies, use of personal electronic devices within the district, electronic communications, use of the district's network, Internet, and social networking tools.

II. General Statement of Policy

District 199 considers its own stated educational mission, goals, and objectives when making decisions regarding employee access to School District technology. Access to the district's network and Internet enables employees to explore libraries, databases, web pages, other online resources, and connect with people around the world. The district expects its instructional staff to blend safe and thoughtful use of the district's network, educational technologies and the Internet throughout the curriculum, providing guidance to students.

District electronic technologies are used for educational purposes. Employees are expected to use electronic technologies to further the district's educational mission, goals and strategic direction. Employees are expected to use the district's electronic technologies to support classroom activities, educational research or professional enrichment.

Use of the district's electronic technologies is a privilege, not a right. The district's network, an educational technology, is a limited forum; the district may restrict speech for educational reasons.

III. Guidelines in Educational Use of Electronic Technologies

Electronic technologies are assets of the school district and are protected from unauthorized access, modification, destruction or disclosure. Use of personal devices, while on district property, is subject to all policies and guidelines, as applicable, plus any state and federal laws related to Internet use, including copyright laws.

A. The district reserves the right to monitor, read or copy any item on or using the district's electronic technologies, including its network.

B. By authorizing use of the district system, the district does not relinquish control over materials on the system or contained in files on the system. Users should not expect privacy in the contents of personal files on the district system.

C. Employees will not vandalize, damage or disable any electronic technology or system used by the district.

D. Routine maintenance and monitoring of electronic technologies, including the district network, may lead to a discovery that a user has violated this policy, another school district policy or the law.

IV. User Notification

Users will be notified of school district policies relating to Internet use. This notification must include:

A. Notification that Internet use is subject to compliance with district policies.

B. Disclaimers limiting the district's liability relative to:

1. Information stored on district media, drives or servers.

2. Information retrieved through district computers, networks or online resources.

3. Personal property used to access district computers, networks or online resources.

4. Unauthorized financial obligations resulting from use of district resources or accounts to access the Internet.

C. A description of the privacy rights and limitations of district sponsored or managed Internet accounts.

D. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data and Policy 515, Protection and Privacy of Student Records.

E. Notification that should the user violate the district's acceptable use policy, the user's access privileges may be revoked, and/or appropriate legal action may be taken.

F. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

V. Unacceptable Uses of Electronic Technologies and District Network

Misuse of the district's electronic technologies may lead to discipline of the offending employee. The following uses of school district electronic technologies while either on/off district property and/or personal electronic technologies while on district property and district network ("electronic technologies") are considered unacceptable:

A. Users will not use electronic technologies to create, access, review, upload, download, complete, store, print, post, receive, link, transmit or distribute:

1. Pornographic, obscene or sexually explicit material or other visual depictions;

2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language;

3. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

4. Materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or threatens the safety of others;

5. Storage of personal photos, videos, music or files on district servers or cloud services. The district does not take responsibility for personal files stored on district technologies.

B. Users will not use electronic technologies to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

C. Users will not use electronic technologies to engage in any illegal act or violate any local, state or federal laws.

D. Users will not use electronic technologies for political campaigning.

E. Users will not use electronic technologies to vandalize, damage or disable the property of another person or organization. Users will not make deliberate attempts to degrade or disrupt equipment, software or system performance. Users will not tamper with, modify or change the district system software, hardware or wiring or take any action to violate the district's security system. Users will not use the district's electronic technologies in such a way as to disrupt the use of the system by other users.

F. Users will not use electronic technologies to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

G. Users must not deliberately or knowingly delete other users files or data.

H. Users will not use electronic technologies to post information in public access areas regarding private or confidential information about another person. Private or confidential information is defined by board policy, state law, and federal law.

1. This paragraph does not prohibit the posting of employee contact information on district web pages.

2. This paragraph does not prohibit communications between employees and other individuals when such communications are made for legitimate education reasons or personnel-related purposes (i.e. communications with parents or other staff members related to students).

3. This paragraph specifically prohibits the use of electronic technologies to post private or confidential information about another individual, employee or student, on social networks, including but not limited to social networks such as “Facebook,” “Twitter,” “Instagram,” Snapchat,” and “Reddit,” and similar websites or applications.

I. Users will not repost or resend a message that was sent to the user privately without the permission of the person who sent the message.

J. Users will not attempt to gain unauthorized access to the district’s electronic technologies or any other system through electronic technologies

K. Users will not attempt to log in through another person’s account, or use computer accounts, access codes or network identification other than those assigned to the user. Users

L. Users must keep all account information and passwords private.

M. Messages and records on the district’s electronic technologies may not be encrypted without the permission of the Director of Instructional Technology.

N. Users will not use electronic technologies to violate copyright laws or usage licensing agreements:

1. Users will not use another person’s property without the person’s prior approval or proper citation;

2. Users will not download, copy or exchange pirated software including freeware and shareware; and

3. Users will not plagiarize works found on the Internet or other information resources.

O. Users will not use electronic technologies for unauthorized commercial purposes or financial gain unrelated to the district’s mission. Users will not use electronic technologies to offer or provide goods or services or for product placement.

P. Use of Unmanned Airborne Vehicles (UAV’s) or drones is prohibited on school property without prior approval of the Director of Instructional Technology or building principal.

VI. Employee Electronic Technologies Use

A. The Employee Device Guidelines and Agreement Form (see Appendix I) for employees must be read and signed by the employee in order to be granted access to district technologies.

B. The Guidelines for Employee Personal Use of Social Networking (see Appendix II) must be read and adhered to by employees engaging in social networking for personal use.

C. Employees will not vandalize, damage or disable any electronic technology or system used by the district.

D. Use of Email

The school district provides access to electronic mail for district communication between district employees and students, families, and the community.

1. The email system will not be used for outside business ventures or other activities that conflict with board policy.

2. All emails received by and sent through district electronic mail system are subject to review by the district.

3. Appropriate language must be used when communicating using the district email system or network.

4. All emails are assumed to be documents that can be disclosed to the public unless the content of the email is protected as private or confidential information under data privacy laws. All information contained in an email must be treated in accordance with Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Student Records regarding student and employee data privacy.

5. All emails to a student's parents or guardians about a student must adhere to the following precautions:

   a. Do not use email to communicate about confidential student information unless the parent or guardian has requested the communication.

   b. Do not put information in an email that you would not put on district letterhead.

   c. Emails containing student information should be sent to the parent or guardian's personal email address unless requested otherwise.

d. A phone call is the means for sharing confidential student information. Do not leave voicemail messages containing confidential information.

6. Employees will not provide access to their email accounts to nonemployees.

7. All emails should include the employee's name and contact information the bottom of the email.

8. A confidentiality statement will be appended to all external email communication.

9. Employees will report inappropriate emails to the media specialist, the employee's supervisor or the director of instructional technology.

10. Emails having content governed by the district's record retention schedule must be kept in accordance with the retention schedule.

VII. Employee Inappropriate Internet Use

Electronic technologies are provided primarily for work-related, educational purposes.

A. Inappropriate use of electronic technologies includes, but is not limited to:

1. Posting, viewing, downloading or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit materials;

2. Posting, viewing, downloading or otherwise receiving or transmitting materials that use language or images that advocate violence or discrimination toward other persons;

3. Posting, viewing, downloading or otherwise receiving or transmitting material that may constitute harassment or discrimination contrary to district policy and state and federal law;

4. Engaging in computer hacking or other related activities;

5. Attempting to, actually disabling or compromising the security of information contained on the district network or any computer;

6. Using encrypted technologies, such as but not limited to VPN, to circumvent the district web filtering system.

7. Engaging in any illegal act in violation of any local, state or federal laws.

B. Employees may participate in public Internet discussion groups using the

electronic technologies, but only to the extent that the participation:

1. Is work-related;

2. Does not reflect adversely on the district;

3. Is consistent with district policy; and

4. Does not express any position that is, or may be interpreted as, inconsistent with the district's mission, goal or strategic plan.

C. Employees may not use the district network or electronic technologies to post unauthorized or inappropriate personal information about another individual on social networks, including but not limited to social networks such as "Facebook," "Twitter," "Instagram," Snapchat," and "Reddit," and similar websites or applications.

D. Employees will observe all copyright laws. Information posted, viewed or downloaded from the Internet may be protected by copyright. Employees may reproduce copyrighted materials only in accordance with Policy 622, Copyright Policy.

VIII. Employee Responsibilities

A. Employees who are leaving positions must leave all work-related files and electronic technologies, including form letters, handbooks, databases, procedures, and manuals, regardless of authorship, for their replacements.

B. Individual passwords for electronic devices are confidential and must not be shared.

1. If an employee's password is compromised or learned by another person, the password should be changed immediately.

2. An employee is responsible for all activities performed using the employee's password.

3. No employee should attempt to gain access to another employee's documents without prior express authorization.

4. Any device with access to private data must not be left unattended and must be protected by password protected screen savers.

C. Employees are expected to use technology necessary to perform the duties of their position.

D. Employees will care for all district issued technologies as outlined in the Employee Device Guidelines and Agreement (see Appendix I).

E. Employees who fail to adhere to district policy are subject to disciplinary action in accordance with their collective bargaining agreement or contract. Disciplinary action may include suspension or withdrawal of Internet or email access, payment for damages or repair, termination and/or referral to civil or criminal authorities for prosecution.

IX. Guest Access and Internet Use

A. Guest access to the school district's open wireless network is provided as a service to the community, and is subject to all district policies and guidelines, plus any state and federal laws related to Internet use, including copyright laws.

B. Guest access is filtered and provides limited bandwidth. Some services may be blocked and/or filtered.

C. Limited technical support is provided for guest access and is identified in the service level agreement found on the district technology website.

X. Records Management and Archiving

All technological data is data under the Minnesota Government Data Practices Act, the Family Educational Rights and Privacy Act, Records Retention Schedule, and school board policy.

XI. Filter

A. With respect to any of its electronic technologies with Internet access, and personal devices accessing the school district network, the district will follow the guidelines provided by the Children's Internet Protection Act, and will monitor the online activities of users and employ technology protection measures during any use of such electronic technologies by users. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;

2. Child pornography; or

3. Harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; or

2. Depicts, describes, or represents, in a patently offensive way with respect

to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks value to minors.

C. Disclaimer limiting the district's liability

The district uses technical means to filter Internet access however, this does not provide foolproof means for enforcing the provisions of this acceptable use policy.

XII. Liability

Use of the school district's educational technologies is at the user's own risk. The system is provided on an "as is, as available" basis. The district will not be responsible for any damage users may suffer. The district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system, nor is it responsible for damages or injuries from improper communications or damage to property used to access school computers and online resources. The district will not be responsible for financial obligations arising through unauthorized use of the district's educational technologies or the Internet.

XIII. Implementation and Policy Review

A. The school district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy. These guidelines, forms and procedures will be an addendum to this policy.

B. The administration will revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The district educational technologies policy is available for review by parents, employees and members of the community.

D. Due to the rapid evolution in educational technologies, this policy will be reviewed annually.

Legal References:
15 U.S.C. § 6501 et seq. – Children's Online Privacy Protection Act
17 U.S.C. § 101 et. seq. – Copyrights
20 U.S.C. § 6751 et seq. – Enhancing Education through Technology Act of 2001
47 U.S.C. § 254 - Children's Internet Protection Act of 2000 (CIPA)
47 C.F.R. § 54.520 - FCC rules implementing CIPA
Minn. Stat. § 121A.031 – School Student Bullying Policy
Minn. Stat. § 125B.15 – Internet Access for Students
Minn. Stat. § 125B.26 – Telecommunications/Internet Access Equity Act
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969)

United States v. American Library Association, 539 U.S. 194 (2003)
Doninger v. Niehoff, 527 F.3d 41 (2nd Cir. 2008)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, No. 12-588, 2012 WL 3870868 (D. Minn. 2012)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other grounds 816 N.W.2d 509 (Minn. 2012)
S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)
Kowalski v. Berkeley County Sch., 652 F.3d 565 (4th Cir. 2011)
Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3rd Cir. 2011)
Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist., 853 F.Supp.2d 888 (W.D. Mo. 2012)
M.T. v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007)

Cross References:
Policy 403 - Discipline, Suspension, and Dismissal of School District Employees
Policy 406 - Public and Private Personnel Data
Policy 505 - Distribution of Non-school Sponsored Materials on School Premises by Students and Employees
Policy 506 - Student Discipline
Policy 514 - Bullying Prohibition Policy
Policy 515 - Protection and Privacy of Student Records
Policy 519 - Interviews of Students by Outside Agencies
Policy 521 - Student Disability Nondiscrimination
Policy 522 - Student Sex Nondiscrimination
Policy 524 - Student Electronic Technologies Acceptable Use
Policy 603 - Curriculum Development
Policy 604 - Instructional Curriculum
Policy 606 - Textbooks and Instructional Materials
Policy 806 - Crisis Management Policy
Policy 904 - Distribution of Materials on School District Property by Nonschool Persons
Elementary and Secondary Student Expectations Handbooks

Appendix I to Policy 424

EMPLOYEE DEVICE GUIDELINES AND AGREEMENT

Inver Grove Heights Schools provides staff the use of district devices, including but not limited to laptops, tablets, and smartphones, for use inside and outside the workplace in order to enhance, enrich, and facilitate teaching, administrative duties, and work-related communications. The District's digital devices are to be used as a productivity tool for education-related business, curriculum enhancement, research, and communications. Staff members may use the District's digital devices for limited personal purposes subject to these guidelines and the **Electronic Technologies Acceptable Use Policy 424**.

- Staff members should use professional judgment when using the District's technology. All laptops and related equipment and accessories are District property and are provided to the staff members during their employment with the District. As a condition of use of the District's laptop computers and other devices, staff members must abide by the following:
    - I will not attempt to install software or hardware or change the system configuration, including network settings, without prior consultation with school or District technology personnel.
    - I will protect District laptops and devices from damage and theft.
    - I will not be held responsible for computer and device problems resulting from school-related use.
    - I will be held personally responsible for any problems caused by negligence or unacceptable use as outlined in Policy 424 or these guidelines.
    - I will not dispose of District laptops, cell phones, tablets, chromebooks, or associated charging devices no matter the condition (even broken or inoperable).
    - In case of non-renewal, leave, retirement, resignation, etc., I will return my laptop, district devices, power adapters, and other accessories to the District Instructional Technology Department or my school's media center.

Data Privacy

The protection and privacy of data on all District devices is articulated in the following policies:

- Policy 406 Public and Private Personnel Data
- Policy 409 Employee Publications, Instructional Materials, Inventions and Creations
- Policy 515 Protection and Privacy of Student Records
- Policy 424 Employee Electronic Technologies Acceptable Use

The following items should be set up on all District devices to ensure security:

- A strong password for all accounts and devices
- A screen lock with passcode in order to access the device
- AutoLock on all devices (recommended not to exceed 15 minutes)

How to Avoid Laptop Computer and Device Theft

- Never leave District devices in plain sight. Do not leave devices in a vehicle, even if the vehicle is in your driveway or garage.
- Carry your laptop in a nondescript carrying case or bag when traveling.
- Always take your laptop with you when leaving a meeting or conference room.

- Lock the laptop in your office or classroom during off-hours or in a locked cabinet or desk when possible.

What to Do in Case of Theft or Loss

Employees should follow these steps if their technology device is lost or stolen:

- Immediately report the incident to your immediate supervisor and the Instructional Technology Department.
- If on hand, the Instructional Technology Department will provide you with your device's make, model, serial number, and estimated value for police and insurance purposes.
- File/Obtain an official police report documenting the theft or loss.
- Report thefts to your personal insurance provider, if applicable.
- Provide a copy of the police report to the Instructional Technology Department.
- The Instructional Technology Department will work with your building to provide a replacement device.

General Device Care

- Adhesive decorations, including stickers, should not be placed on District laptops or devices.
- Screens can be cleaned with dry microfiber cloths or tech device alcohol wipes. Liquid cleaners should never be used on devices.
- Keep food and all liquids away from devices to avoid damage.
- Anything placed on District-owned property must abide by district guidelines.
- Only charge devices with manufacturer issued chargers distributed by the District tech department.
- Cost of replacing laptop power cords is $80.

Acceptable Use Reminders

- Electronic technologies are provided primarily for work-related, educational purposes.
- Individual passwords are confidential and must not be shared.
- Any device with access to private data must not be left unattended and must be protected by password-protected screensavers.
- District technologies are intended to only be used by District employees.

I have read the Employee Device Guidelines and District Policy 424 titled Electronic Technologies Acceptable Use. I understand and will abide by the Employee Device Guidelines for all district devices issued to me and District Policy 424 titled Electronic Technologies Acceptable Use.	
Employee's Name:	**District Building Location:**
Employee's Signature:	**Date:**

Appendix II to Policy 424

GUIDELINES FOR EMPLOYEE PERSONAL USE OF SOCIAL NETWORKING

The District recognizes the importance of the online social media networks as a communication and e-learning tool and provides password protected social media tools and district approved technologies for e-learning, communication, and collaboration among employees. Public social media networks, outside of those sponsored by the District, may not be used for classroom instruction or school-sponsored activities without the prior authorization of the Superintendent or his/her designee. Parental consent must also be obtained for student participation in social networks. The District may use these tools and other communication technologies in fulfilling its responsibilities for effectively communicating with the general public**.**

I. Definitions

A. "Public online social media" are defined to include: websites, web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other interactive social media available to the public via the Internet.

B. "District approved, password protected online social media" are defined as interactive media within the District's electronic technology networks or which the District has approved for educational use. Technologies outside of the District's network may also be approved for educational use if limited to instructional content selected according to the textbook and instructional material policy and procedures and used according to the requirements of the policy. The District has greater authority and responsibility to ensure the safety or our students and can limit public access within this forum.

II. Requirements

District staff members are expected to serve as positive ambassadors for the District and appropriate role models for students. It is vital that staff maintain professionalism in their interactions with students and the community. Failure to do so could put staff members in violation of existing district policy and at risk of disciplinary action. The District requires employees to observe the following rules when referring to the District, its schools, students, programs, activities, employees, volunteers, and communities on any social networks:

A. Comply with all state and federal laws and any applicable district policies when engaging in use of social media network. Those laws, policies and rules include but are not limited to Minnesota statutes and district policies regarding employee-student relationships, harassment and violence, bullying, hazing, mandatory reporting, data privacy, internet acceptable use, advertising prohibitions, code of ethics, and copyright and fair use regulations.

B. When employees choose to join or engage with District students, families, or fellow employees in a social media context that exists outside those approved by the District, they are advised to maintain their professionalism as District employees and have responsibility for addressing inappropriate behavior or activity on these networks, including requirements for mandated reporting.

C. Employees have responsibility for maintaining appropriate employee-student relationships at all times including:

1. Using professional judgment when necessary for the safety of students online and responding appropriately as a mandated reporter when applicable. Every

school district employee is to maintain a standard of professionalism and act within accepted standards of conduct and applicable standards of ethics and professional conduct in Minnesota law. Each school district employee is expected to exercise good judgment and professionalism in all interpersonal relationships with students including through the use of social media.

2. Communications with students or former students who are minors on social media must be only for school-related purposes and through the use of School District sponsored social media networks. While it may be acceptable for employees to "friend" relatives or children of close friends on personal social media networking sites, communication when there is teaching, coaching, or other school relationship must be limited to School District sponsored social media networks. Employees may not inform, publish, or distribute to students any personal social networking site of the employee.

3. Excessive informal and social involvement through social media with individual students is prohibited. Such communication is unprofessional, is not compatible with employee-student relationships, and is inappropriate. Unprofessional relationships include writing personal letters, email or text messages; calling students on cell phones or allowing students to make personal calls unrelated to class work or school activities; sending inappropriate pictures to students; discussion or revealing personal matters about a staff member's private life or inviting students to do the same; engaging in sexualized dialogue in any form.

D. Accept personal responsibility for content, whether purposeful or inadvertent. Employees shall not use obscene, profane, or vulgar language on any social media network or engage in communications or conduct that is harassing, threatening, bullying, libelous, or defamatory or that discusses or encourages any illegal activity or the inappropriate use of alcohol, use of illegal drugs, sexual behavior, or sexual harassment.

E. Employees may not disclose information on any social media network that is confidential or proprietary to the District, its students, or employees or that is protected by data privacy laws.

1. Employees shall not post photos or movies to public sites that include students without parent consent.
2. Employees shall not post photos or movies to public sites that include fellow employees without their consent.

3. Employees shall not post photos or images of non-public district premises and property, including floor plans without expressed written consent of the Superintendent.

F. Any views expressed on a public online social media site do not reflect the views of the District.

1. Employees may not act as a spokesperson for the District or post comments as a representative of the District, except as authorized by the Superintendent or his/her designee.

2. Employees may not post or use the District or building logo on any public online social media site without permission from the Superintendent, building principal, or building designee.

3. When employees, including coaches/advisors, choose to join or engage with social networking groups of student groups within the District, they do so as an employee of the District and will annually disclose the existence of and their participation in such networks.

G. School District Action

An employee who is responsible for a social media network posting that fails to comply with the rules and guidelines set forth in this policy may be subject to discipline, up to and including termination. Employees will be held responsible for the disclosure, whether purposeful or inadvertent, of confidential or private information, information that violates the privacy rights or other rights of a third party, or the content of anything posted on any social media network.

H. Limited Expectation of Privacy

Employees should expect only limited privacy in the contents of district sponsored social media tools or social media accessed by employees on district equipment. Routine maintenance and monitoring of the District's system may lead to a discovery that a user has violated this policy, another district policy, or the law. An individual investigation or search also will be conducted if district authorities have a reasonable suspicion that the search will uncover a violation of law or district policy. The District also will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with district policies conducted through the district systems. In addition, parents have the right at any time to investigate or review the contents of student's files, which may include materials posted through district-sponsored social media tools or social media accessed through district equipment.

Employees should be aware that the District retains the right at any time to investigate or review the contents of these district social media networks. In addition, employees should be aware that data and other materials in files maintained on district systems may be subject to review, disclosure, or discovery under Minn. Stat.ch 13 (the Minnesota Governmental Data Practices Act). The District also may at any time review any social media network or communication made public by the employee or other individuals regarding the employee.

These guidelines will not be construed or applied in a manner that improperly interferes with an employee's right under the National Labor Relations Act.