
**INVESTIGATION OF SCHOOL EMPLOYEE
MISCONDUCT INVOLVING THE
MISUSE OF TECHNOLOGY**

**2003 ELA Convention
Savannah, Georgia**

**Jeffrey J. Horner
Bracewell & Patterson, L.L.P.
711 Louisiana, Suite 2900
Houston, Texas 77002**

**713-221-1219 – telephone
713-222-3257 – fax**

jeffrey.horner@bracepatt.com

INVESTIGATION OF SCHOOL EMPLOYEE MISCONDUCT INVOLVING THE MISUSE OF TECHNOLOGY

1. INTRODUCTION

Technology in the workplace has increased significantly in recent years, including the introduction of e-mail, voicemail, facsimile machines, the Internet, and sophisticated computer software. Employers are frequently confronted with the need to investigate allegations that employees are involved in misconduct relating to the use of technology, and take appropriate action when the investigation uncovers wrongdoing. Due to the application of various state and federal statutes and constitutional provisions, the importance of fair and objective investigations is even more pronounced in the public school setting. This outline outlines the legal setting in this area, and provides practical tips for handling investigations relating to the misuse of technology by employees.

2. LEGAL SETTING

Public school districts are political subdivisions of the state. Thus, their activities constitute "state action" for constitutional purposes. This means federal constitutional guarantees both protect and constrain public school officials and employees. These same guarantees do not apply to private educational institutions.

Regardless of whether your institution is public or private, managing employees in this legal setting begins with the promulgation of policies and procedures to ensure fairness and compliance with the law. Courts generally review claims by determining the existence of any policies and procedures and, if they exist, whether they were followed. If these inquiries are satisfied, administrators and educational entities stand a significantly better chance of having their decisions supported in court.

It is important to note that achieving fairness in the workplace does not mean that employees accused of wrongdoing are entitled to all the formal standards applicable to investigation and prosecution in the criminal setting. To the contrary, courts have generally recognized a distinction between the criminal setting and the employment context. The U.S. Supreme Court recognizes that a public employer has a substantial interest in investigating misconduct by employees in an informal manner that does not impose significant administrative burdens or intolerable delays.¹

Another legal consideration for public schools in the investigatory realm involves due process standards. The U.S. Supreme Court outlined the general requirements for providing pre-termination due process to public employees in *Loudermill v. Cleveland Board of Education*.² Under *Loudermill*, public employees are entitled to: (1) oral or written notice of the charges against them; (2) an explanation of the employer's evidence; and (3) an opportunity for the accused to present his or her side of the story.³ In this analysis, the Court presumed that a post-termination hearing would follow. The process due private employees will depend upon the policies of the particular institution.

¹ O'Connor v. Ortega, 480 U.S. 709 (1987).

² 470 U.S. 532 (1985).

³ *Id.* At 546.

A final consideration in investigations is the need for clearly articulated, reasonable standards of conduct set forth in employee handbooks. The handbooks should include any applicable policies and procedures. Furthermore, the handbook must be careful to follow school policy and not to inadvertently convert an "at-will" employment relationship into a constitutionally protected property right to continuous employment.

3. INVESTIGATIONS RELATING TO THE MISUSE OF TECHNOLOGY

As noted above, in recent years a proliferation of technological advances has permeated the school setting. The possibility of abuse of technology in the school setting is very real. Therefore, school administrators must be aware of possible areas of abuse or misuse of technology, and be prepared to react accordingly.

A. *Initial Considerations*

Personal use of school technology, including school computers, can help employees become more knowledgeable about technology. However, excessive personal use clearly interferes with job performance, and can sometimes violate the law. For example, some personal e-mail communications can be inappropriate and unacceptable for the school environment. Furthermore, although the Internet is a useful tool to secure information on a variety of subjects, viewing and downloading of inappropriate materials, such as pornographic material, cannot be permitted. Educational institutions have substantial discretion in preventing or regulating personal use of their computers. This section will address some of the legal issues relating to the misuse of technology.⁴

B. *Statutes Relating to Misuse of Technology*

To a great extent, the primary legal issue on the misuse of technology relates to privacy. As *O'Connor v. Ortega* indicated, an employee has a "reasonable expectation of privacy" in the contents of his or her office.⁵ However, this expectation of privacy is not unfettered, and school officials may make a search of individual belongings at school, including his or her computer files, if "reasonable suspicion" exists to determine that a violation of the law or school rules has occurred.⁶ Various statutes relate to the possible misuse of technology.

- **Electronic Communications Privacy Act**

The Electronic Communications Privacy Act ("ECPA") was passed in the late 1980's as an amendment to the Federal Wire Tap Act.⁷ The ECPA protects the privacy of electronic communications, including e-mail. It criminalizes the interception of electronic messages, such as e-mail, while in transit.⁸ The ECPA

⁴ The author wishes to recognize the contributions of Mr. Bruce Smith of Drummond Woodsum & McMahon, an attorney from Portland, Maine, in the drafting of this outline. In particular, Mr. Smith's article in the August 2001 issue of National School Board Association's *Inquiry & Analysis* was very helpful in drafting this outline.

⁵ 480 U.S. at 719-720.

⁶ *Id.* At 725-726.

⁷ See 18 U.S.C. §§ 2510-2522.

⁸ See 18 U.S.C. § 2511; see also *Steve Jackson Games Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994).

contains an exception for the provider of the electronics communication service. In most cases, educational institutions will fit this exception. In general, the ECPA is not a significant obstacle to school monitoring of employee e-mail communications.

- **Family Educational Rights and Privacy Act**

The Family Educational Rights and Privacy Act ("FERPA")⁹ relates to student educational records at any schools, whether public or private, which receive federal funding. Generally, an employee cannot misuse or unlawfully disseminate student records without violating FERPA. Of course, when a school employee is required to use student records as part of his or her job duties, FERPA would not be violated. However, the inappropriate dissemination of student records by school employees could subject an employee to adverse employment action or even civil liability.¹⁰ One recent U.S. Supreme Court case held that school districts cannot be held liable for monetary damages under FERPA.¹¹

- **Communications Decency Act**

In 1996, the U.S. Congress passed the Communications Decency Act ("CDA").¹² One provision of this statute permits blocking and filtering software to restrict student and employee access to inappropriate on-line material at school.¹³

- **Children's Internet Protection Act**

The Children's Internet Protection Act ("CIPA") requires schools to restrict employee and student access to the Internet.¹⁴ Under the CIPA, covered schools must have an Internet safety program which filters both adult and student access to visual depictions that are obscene or constitute child pornography. The program must also prevent students from accessing materials that are harmful to minors.¹⁵

- **A Recent Case in Point**

A Second Circuit Court of Appeals case illustrates the balancing act which courts must undertake regarding the misuse of employee technology. In *Leventhal v. Knapek*,¹⁶ based on an anonymous tip, a school supervisor sought

⁹ 20 U.S.C. § 1232g *et seq.*

¹⁰ *See* *Fay v. South Colonie Central School District*, 802 F.2d 21 (2d Cir. 1986).

¹¹ *Doe v. Gonzaga Univ.*, 122 S.Ct. 2268 (2002).

¹² 47 U.S.C. § 230, *et seq.*

¹³ *See* 47 U.S.C. § 230(b)(4).

¹⁴ Pub. L. 106-554 § 1(a)(4).

¹⁵ *Id.*

¹⁶ 266 F.3d 64 (2d Cir. 2001).

evidence for the alleged unauthorized use of computer equipment by searching the employee's office and computer files. The court recognized that the employee had a reasonable expectation of privacy in his computer. However, the court held that the supervisor had a reasonable basis for the search.¹⁷ This case illustrates the permissible actions of school officials when confronted with reasonable suspicion of technology misuse.

4. GUIDANCE FOR EMPLOYEE USE OF SCHOOL TECHNOLOGY

Schools should establish a written set of rules or policies relating to the use of school technology, including school computers and Internet connections. These rules will reduce the misuse of the computer system and provide a foundation for investigation and discipline as discussed earlier in this paper. School rules and policies should address at least the following areas:

A. *Personal Use*

School districts should restrict computer networks and Internet connections to purposes related to job performance. Personal use should at the very least be restricted or, if necessary, disallowed completely.

B. *Confidentiality*

Employees should be directed not to transmit confidential information concerning students or others; these transmissions could violate FERPA. Schools may want to consider purchasing secure systems to safeguard information which is not subject to open records laws, particularly student records.

C. *Non-Privacy Statement*

A policy should directly state that all data in school computers and the computer networks themselves are considered school business and subject to being monitored; employees should have no right to privacy in their computer files.

D. *Illegal Uses*

A policy should identify categories of illegal uses and state that an individual can be subject to adverse employment action, including termination, for such illegal uses.

E. *Advertising and Solicitation*

A policy should prohibit advertising and solicitation on school computers by outside groups. The policy should be written broadly to apply to employees, students, and anyone who might have outside access to school computers.

F. *Account Safeguarding and Passwords*

Employees should be reminded that they are responsible for safeguarding their own passwords; they will be held accountable for the consequences of intentional or

¹⁷ *Id.* at 72.

negligent disclosure of this information. Employees should also be required to "log off" at the end of each workday.

G. *Role of the Technology Coordinator*

Each school should appoint a person to coordinate and police the district's technology system. The duties of this individual should include implementation of the technology policies. Employees should be reminded to contact this person in the event they have questions regarding the policies. Furthermore, employees should be instructed to report all violations of this policy to the technology coordinator, and to assist the coordinator in any investigation regarding possible misuse of technology.

5. CONCLUSION

Assuring that employees are treated fairly when they are accused of wrongdoing starts with a carefully planned, timely, and impartial investigation. The relaxed standards of reasonable suspicion apply, as opposed to criminal law standards. The investigation should be conducted in a manner which allows any wrong to be detected while protecting the rights of the accused. Regarding technology, policies should be developed in writing to guide employee conduct.

Investigators should treat people with whom they come into contact in the same manner they would expect to be treated in a similar situation. Follow the "Golden Rule." Care must be exercised to avoid trampling on the dignity of an accused. By doing so, the objective of the investigation can be obtained, and the school can continue to function efficiently after the investigation is complete.

Jeffrey J. Horner is a partner at the Houston, Texas law firm of Bracewell & Patterson, L.L.P. He is head of the firm's Public Law Section, and has specialized in the representation of school districts and colleges for 20 years. Mr. Horner served as president of the Education Law Association in 1998. He is also an adjunct professor of education law at the South Texas College of Law in Houston. Mr. Horner received his law degree from the University of Virginia School of Law.