

Running head: EMAIL COMPLIANCE

Email Compliance and Management in Education

Angela Herring

East Carolina University

DTEC 6865 Fall 2007

## Abstract

This paper will examine email management practices and the impact government regulations pose on educational institutions. Along the way we will look at effective ways to introduce compliance strategies into an email management plan.

The responsibility of email management from a security standpoint is a textbook case for incorporating the well-known CIA triad as an information security strategy. Responsibilities include “keeping email messages *confidential*, maintaining the *integrity* of the application, and ensuring that records of communication are *available* for some period of time.” (Sullivan, 2006) If an institution incorporates sound email management practices in the areas of email security and policy, this will in turn encompass compliance issues.

The regulation that has the most significant impact on email management for educational institutions is FERPA, the Family Educational Rights and Privacy Act, which “is a Federal law that protects the privacy of student education records.” (FERPA)

## Email Compliance and Management in Education

### COMPLIANCE

Compliance is a hot topic in all areas of information security at the moment, with email management being no exception. Many laws and legislation currently dot the information security horizon with Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, and PCI being the so-called big boys of the information security compliance game. However these acts have little influence on public educational institutions with regards to email management. So what law does an educational institution need to be concerned about? FERPA.

FERPA is the Family Education Rights and Privacy Act of 1974. FERPA was designed to protect the privacy of student education records. There are two types of educational records defined by FERPA. Directory and Non-directory or protected information. Directory information may be disclosed by the educational institution without written consent of the student.

Directory information may include:

- Name
- Address
- Phone number and email address
- Dates of attendance
- Degrees awarded
- Enrollment status
- Major field of study

Non-directory or protected information may not be released to anyone without written consent of the student. It should also not be accessed by faculty or staff unless they have a legitimate academic need to do so. Non-directory or protected information may include:

- Social security numbers
- Student identification number
- Race, ethnicity, and/or nationality

- Gender
- Transcripts and grade reports (Van Dusen)

Representatives of the school “must have written permission from the parent or eligible student in order to release any information from a student’s education record.” (FERPA)

Following are the circumstances where educational records can be disclosed to a third party without written consent:

- School officials with legitimate educational interest
- Other schools to which a student is transferring
- Specified officials for audit or evaluation purposes
- Appropriate parties in connection with financial aid to a student
- Organizations conducting certain studies for or on behalf of the school
- Accrediting organizations
- To comply with a judicial order or lawfully issued subpoena
- Appropriate officials in cases of health and safety emergencies
- State and local authorities within a juvenile justice system pursuant to specific State law (FERPA)

Email has become such a commonplace method of communication in many organizations that its implications are often taken for granted. It is easy enough not to “speak” or “photocopy” information protected by FERPA, but employees need to realize that sending protected information via email has far reaching consequences. Even if the person the information was sent to has a legitimate need to access the information, it needs to be considered that this information may be intercepted while it is in transit. The email may be easily forwarded to another party. The email may be archived on any number of servers it traversed in its route to its final destination. The system that the email was accessed on may not be secure, or it may be the victim of tampering or even theft. (Electronic Records Management Guidelines, 2005) Email brings a whole other aspect to the game when dealing with FERPA privacy issues. This is where an effective email management plan comes into play.

## MANAGEMENT

Although email was originally intended for asynchronous communication, it has evolved into a delivery mechanism that supports the following tasks (to name a few): document delivery and archiving, work task delegation, project management, electronic address book, sending reminders, seeking assistance, scheduling, and handling technical support requests. (Whittaker & Sidner) Each time an employee accesses a company email account, the company assets and reputation are at risk. Whether the risk stems from accidental misuse or intentional abuse, email can cause legal, regulatory, security, and productivity problems. To mitigate these potential risks, companies need to implement a 3-step plan consisting of policy, education, and enforcement. (Flynn)

When writing policy, be sure to keep your audience in mind to ensure that the policy encompasses all levels of users that will be accessing the email system. The overall theme of the email policy should be that email is not private and that it is “considered company property and can be retrieved, examined, and used in a court of law.” (Stack) It is amazing how many people are not aware that sending an email is the equivalent of sending a postcard via the US Postal Service in the respect that anyone along the way that intercepts it is privy to its contents. This leads into the next step of an email management plan, education.

Once policy has been established, the next step is to educate your employees. This should be done using a variety of methods to ensure saturation among email users. It is okay to be repetitive. The new policy should be distributed to employees and employees should be made to sign an agreement form stating that they have read the policy and that they agree to comply with it. After employees have had time to take in the policy, mandatory training should

be held to explain the policy, go over scenarios of what would be considered acceptable and unacceptable use, and answer any questions employees may have regarding the policy and/or the consequences for non-compliance. The mandatory training sessions are a good time to tie in any state or federal regulations that the policy is designed to enforce. Some best practices of implementing new email policy include (1) disabling email access until employees have completed the mandatory training, and (2) distributing short quizzes after the training requiring an 80% pass rate before email access will be restored. (Flynn) The most important thing to understand is that the education phase of policy implementation is an ongoing process. It will need to be provided every time a new hire is added and will need to be repeated periodically as technology changes or issues arise that would cause the policy to be revised. Part of the ongoing education should include awareness messages either in the form of a newsletter, an email (how ironic), or posters placed in strategic places around the company. These awareness messages should focus on different parts of the email policy and include the consequences of failing to abide by the policy. Humor is a good tool to implement into this part of the education phase. Here are some sample email security awareness posters from a company called NoticeBored [http://www.noticebored.com/html/sep\\_07\\_posters.html](http://www.noticebored.com/html/sep_07_posters.html) that offers a monthly subscription including posters like these, along with a comprehensive package of high quality security awareness materials. (Email Security Posters)



Policy enforcement is the final major factor in implementing an effective email management program. Technology solutions should be used where appropriate. Stiff consequences should also be in place to deter potential misuse and/or abuse. These consequences can range from dissatisfactory marks on performance appraisals to termination of employment. (Flynn) What ever the disciplinary action is, it should match the offense and be tailored to status of the employee. For example, IT has a greater responsibility for the security of archived email than a casual user. The consequences for misuse should reflect that increased responsibility.

Following are sample use policies pertaining to Email Usage and Email Retention. These policies were retrieved from <https://www2.sans.org/resources/policies/#template> and may be modified to fit your organizations needs. (The SANS Security Policy Project)

## EMAIL USAGE POLICY

### 1.0 Purpose

To prevent tarnishing the public image of <COMPANY NAME>. When email goes out from <COMPANY NAME> the general public will tend to view that message as an official policy statement from the <COMPANY NAME>.

### 2.0 Scope

This policy covers appropriate use of any email sent from a <COMPANY NAME> email address and applies to all employees, vendors, and agents operating on behalf of <COMPANY NAME>.

### 3.0 Policy

**3.1 Prohibited Use.** The <COMPANY NAME> email system 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 <COMPANY NAME> employee should report the matter to their supervisor immediately.

### 3.2 Personal Use.

Using a reasonable amount of <COMPANY NAME> resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a <COMPANY NAME> email account is prohibited. Virus or other malware warnings and mass mailings from <COMPANY NAME> shall be approved by <COMPANY NAME> VP Operations before sending. These restrictions also apply to the forwarding of mail received by a <COMPANY NAME> employee.

### 3.3 Monitoring

<COMPANY NAME> employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. <COMPANY NAME> may monitor messages without prior notice. <COMPANY NAME> is not obliged to monitor email messages.

### 4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### 5.0 Definitions

Term	Definition
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to <COMPANY NAME> or its customers' reputation or market standing.
Virus warning	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and

contain bogus information usually intent only on frightening or misleading users.

Unauthorized Disclosure      The intentional or unintentional revealing of restricted information to people, both inside and outside <COMPANY NAME>, who do not have a need to know that information.

## 6.0 Revision History

### EMAIL RETENTION POLICY

#### 1.0 Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

#### 2.0 Scope

This email retention policy is secondary to <Company Name> policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All <Company Name> email information is categorized into four main classifications with retention guidelines:

- Administrative Correspondence (4 years)
- Fiscal Correspondence (4 years)
- General Correspondence (1 year)
- Ephemeral Correspondence (Retain until read, destroy)

#### 3.0 Policy

##### 3.1 Administrative Correspondence

<Company Name> Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox admin@<Company Name> has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

### **3.2 Fiscal Correspondence**

<Company Name> Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@<Company Name> has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

### **3.3 General Correspondence**

<Company Name> General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

### **3.4 Ephemeral Correspondence**

<Company Name> Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

### **3.5 Instant Messenger Correspondence**

<Company Name> Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address.

### **3.6 Encrypted Communications**

<Company Name> encrypted communications should be stored in a manner consistent with <Company Name> Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

### **3.7 Recovering Deleted Email via Backup Media**

<Company Name> maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

## **4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## **5.0 Definitions**

### **Approved Electronic Mail**

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here...]. If you have a business need to use other mailers contact the appropriate support organization.

### **Approved Encrypted email and files**

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within <Company Name> is done via a license. Please contact the appropriate support organization if you require a license.

### **Approved Instant Messenger**

The Jabber Secure IM Client is the only IM that is approved for use on <Company Name> computers.

### **Individual Access Controls**

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the `chmod` command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

### **Insecure Internet Links**

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

### **Encryption**

Secure <Company Name> Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

## **6.0 Revision History**

28 July, 2003 Added discussion of backup media

## **CONCLUSION**

After examining how FERPA affects email, and policy, education, and enforcement strategies, the only thing left to discuss regarding an email management plan is the specific security threats and issues that concern IT. Up until now we have been discussing email management from a user perspective, but the IT side has just as much at stake, if not more, in their role as administrators of the email system. Some of the issues include how to prevent and respond to viruses and malware distributed through email; how to prevent unauthorized access to user accounts; how to protect physical access to the email server; and what sort of backup and archival plan is in place and how is it secured. "Policy should clearly define the roles and

responsibilities that managers, network administrators, technical staff, records management staff, support staff, and users will have in the management of email.” (Electronic Records Management Guidelines, 2005)

ITManagement.com states that the top 5 email management issues are spam, compliance, archive search and retrieval, viruses and spyware, and content security. Startling statistics have put email management at the top of many IT Departments to-do lists. In June 2006 approximately 5 billion spam messages were sent per day. That number rose to 86 billion per day in November 2006. That is a 1700 percent increase in just 5 months. Add to this that the average worker generates 14 MB of data per day in email storage, multiplied by the number of employees, times the number of days your company operates a year, and you have got a massive storage issue. (Top 5 Email Management Issues, 2007) When you couple this issue with lost productivity from employees checking personal email accounts, or worse yet using their work email account for personal use, it is not hard to see that email management is not something to be taken lightly. Let me leave you with this final thought. Your email management plan is only as effective as the thoroughness of your email usage policy, the effectiveness of your education, training, and awareness program, and the consistency of policy enforcement and violation consequences.

## References

- \**Electronic Records Management Guidelines*. (2005, March). Retrieved November 25, 2007, from South Carolina Department of Archives and History: <http://www.state.sc.us/scdah/erg/ermEMM.pdf>
- Email Security Posters*. (n.d.). Retrieved November 25, 2007, from NoticeBored: [http://www.noticebored.com/html/sep\\_07\\_posters.html](http://www.noticebored.com/html/sep_07_posters.html)
- FERPA*. (n.d.). Retrieved June 3, 2007, from U.S. Department of Education: <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- Flynn, N. (n.d.). *Ten Easy Steps for Email and Web Best Practices*. Retrieved September 16, 2007, from Message Labs: [http://i.i.com.com/cnwk.1d/html/itp/MessageLabs-Ten\\_Easy\\_Steps\\_Email\\_Web\\_Best\\_Practices.pdf](http://i.i.com.com/cnwk.1d/html/itp/MessageLabs-Ten_Easy_Steps_Email_Web_Best_Practices.pdf)
- Stack, L. (n.d.). *12 Tips for Better E-mail Etiquette*. Retrieved September 16, 2007, from Microsoft.
- Sullivan, D. (2006, October 20). *Email Compliance and Regulations*. Retrieved September 16, 2007, from Realtime Messaging and Web Security: [http://i.i.com.com/cnwk.1d/html/itp/mcafee\\_EmailComplianceRegs.pdf](http://i.i.com.com/cnwk.1d/html/itp/mcafee_EmailComplianceRegs.pdf)
- The SANS Security Policy Project*. (n.d.). Retrieved November 25, 2007, from SANS Institute: <https://www2.sans.org/resources/policies/#template>
- Top 5 Email Management Issues*. (2007, January 4). Retrieved November 25, 2007, from IT Management: <http://www.itmanagement.com/features/top-5-email-management-issues/>
- \*Van Dusen, W. (n.d.). *FERPA: Basic Guidelines for Faculty and Staff A Simple Step-by-Step Approach For Compliance*. Retrieved November 24, 2007, from National Academic Advising Association: <http://www.nacada.ksu.edu/Resources/FERPA-Overview.htm>
- \*Whittaker, S., & Sidner, C. (n.d.). *Email Overload: Exploring Personal Information Management of Email*. Retrieved November 25, 2007, from Lotus Development Corporation: <http://dis.shef.ac.uk/stevewhittaker/emlch96.pdf>