# Google Applications

# Is there a statutory responsibility to protect our students' private information from Google?

**In summary,** prior to deciding on a solution for student email, our investigating committee verified that the confidentiality of our Students, Faculty, and Staff would be protected regardless of the applications decided upon. Googles terms of service explicitly state that they do not own our Students emails.

**In detail**, the primary privacy concerns were brought up due to Google's use of email content to generate advertisements. In the Google Apps for Education services, these advertisements are disabled, but may be enabled in a University's preferences if they choose to do so, we have not and will not enable this for current students.

In addition, in some ways, Google has some stronger legal requirements with regards to the data than Florida Tech does.  The primary example of this is the Electronic Communications Privacy Act. Under this law, Google is typically considered a public network, and requires a legal order or subpoena to release the content of email communications to law enforcement.  Florida Tech, on the other hand, may at its discretion release this information to law enforcement personnel without the need for a legal order or subpoena. However, in general we require legal orders or subpoenas to release the details of these communications.

Google's terms of service state that confidential information will be protected as if it were the entities own confidential data. The agreement with Google is a binding agreement (contract) and they treat all data stored on their systems by our users as confidential. This is actually defined in the agreement.

Here are the relevant sections from the Google terms of service for Education (Accessible at: http://www.google.com/apps/intl/en/terms/education_terms.html )

6.1 Obligations. Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its affiliates, employees and agents in violation of this Section.

....

7.1 Intellectual Property Rights. Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.
....

Confidential Information means information disclosed by a party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is Customer's Confidential Information.

Customer Data means data, including email, provided, generated, transmitted or displayed via the Services by Customer or End Users."

Google may revise their terms and give us 30 days to accept the new terms. This notification must be made in writing. If we reject the terms, the original contract terms are applied for the length of our current agreement. However, upon renewal of the service term, we will need to accept the new terms or terminate our relationship with Google. If we accept the terms, we enter into a new contract.

In addition, the terms specify that if we terminate the agreement, they will delete all of our data after giving us the ability and timeframe from which to export all of the data held by them.

With regards to the confidential information issue, it really depends under what law, policy, or agreement the information falls under. Florida Tech's policy specifically refers to what we consider 'sensitive' information. This is information under which Florida Tech in under legal and regulatory requirements to protect. This includes information covered under the Florida Data-breach notification law (our words), the payment card industry data security standard, specific FERPA protected information, and information the university generally does not want to disclose to protect the privacy of our students, faculty, staff, and guests. This information includes data such as student ID numbers, social security numbers, credit card information, drivers license information, and bank account information.

FERPA is somewhat of an interesting law in which any piece of data that is created as a result of providing educational services is protected under FERPA. For this reason, we do have restrictions on specific FERPA protected data: where it may be stored, who has access to it, how we protect it from inadvertent disclosure and so forth.

With regards to other confidential information, we generally recommend against sending it through email communications, but we do not restrict this. We generally treat email as information that could possibly be seen by others or publicly disclosed. Some examples of this would be sending the information to the wrong email address (auto-completion filling in the wrong person), or a legal action against the University where other individuals or the public may gain access to the contents of those messages.

FERPA defines how the data can be disclosed, but does not restrict it from email communications. However, we take those additional steps to protect certain kinds of information in an attempt to prevent inadvertent disclosure to an individual that does not have an educational need-to-know for the information.

# Google Applications

Unique solution ID: #1159
Author: Tech Support
Last update: 2020-04-13 17:56