Decide What Data to Store in Google Drive

Stephanie Obodda - 2024-04-17 - Comments (0) - Google Drive

We have received questions **whether it is appropriate to use Google Docs for storing and sharing grades or information like tenure committee data**.

There are two essential points to keep in mind in answering this question.

1. The Google Apps we use at Brown is NOT the commercial Google platform. A review by Brown's Information Security Group as well as the security experts in corporations around the world have found that Google Apps is a secure set of tools for most daily work.

2. Like all technology, Google Apps is only as secure as the people and processes behind it. Information stored in Google is secure, just as is information stored in locked file cabinets. When information is shared—whether in print or electronic form—care must be taken.

Appropriate and inappropriate uses of Google Apps

1. As long as appropriate care is taken in sharing information (see below), Google Apps may be used to store and share information such as **grades**. In general, Google Apps is appropriate for most Brown information including Family Educational Rights and Privacy Act (FERPA) protected data and other information that we are not allowed to share broadly.

Historically, grades and other information about students have been shared between the faculty and TAs via email, spreadsheets, and hard copy documents. All of those methods have security concerns and deficiencies. The use of a Google Doc for these purposes has advantages over previously used methods. Remember that only graduate TAs should be granted access to view student grades and that evaluation and grading is the exclusive responsibility of those with a formal instructional appointment. Furthermore, class roster information that includes identifying information about students should **never** be "published to the web," since FERPA guidelines prohibit release of such information outside the confines of the institution.

2. State and federal laws and policies control some types of information for which Google may not currently be certified as appropriate. Examples of these types of controlled information include **social security numbers** as well as federally protected **personal health data** which falls under Health Insurance Portability and Accountability (HIPAA) regulations. A final example of data that would be inappropriate for GAE would be data that falls under the federal International Traffic in Arms (**ITAR**) regulations.

3. **Private documents**: The security of the Google Apps platform is more than sufficient for private documents, such as tenure committee discussions, personal papers, class prep, and research notes. Simply bear in mind the precautions listed below when sharing the document(s) with others. CIS and the University stand behind the security and use of Google Apps, and we encourage its use for most information except where that information is incompatible with GAE due to federal, state or policy regulation. Policies and regulations change, so be cautious; if you are concerned or have questions, feel free to ask for guidance.

Guidelines for sharing data securely

- **Check the email address**: Be sure that you are choosing the proper email address, as there are many similar and duplicate names in our directory. It is also possible to share the document with any individual outside of the organization by simply entering an email address. In any of these scenarios it is essential that you are 100% certain that the entry made is that of the colleague that you intend to share the data with, and that they will use it responsibly.
- **Check the scope of distribution**: choose wisely as to whether you want those you are sharing a document with to have only “view” access, or the ability to edit the document. When you provide someone the ability to “can edit”, they also have the ability to share it with others. Also, be aware of the option to “publish to the web”, and recognize whether the info you are publishing is appropriate for that view.