The BC Data Security Policy defines 3 categories of data -- Public, Internal Use Only, and Confidential.

The Data Security Committee, General Counsel, and the university’s FERPA officer have informally agreed that an additional, 4th category of data will be added to the Data Security Policy that is even more sensitive than “Confidential.” Data that falls in this additional category will not be allowed to be stored off-campus except with written permission (see below). Google Drive is off-campus, and thus data that falls in this category must not be stored on Google Drive. This additional category has not been named yet. Until a formal policy revision is made and approved, you should use the following as a guideline:

- **Public and Internal Use Only.** Acceptable to store on BC Google Drive
- **Confidential.** FERPA data (i.e. student records) is generally defined as Confidential, and can be stored on BC Google Drive, except as noted below. Other Confidential data, except as noted below, can also be stored on BC Google Drive.
- **New Category.** Due to legal restrictions or security concerns, some legally protected and highly sensitive information must not be stored on Google Apps or other “cloud-based” systems without permission of the responsible Vice President or the Provost’s Office. This information, much of which was formerly classified as “Confidential,” includes:
  - Social Security Numbers
  - Financial or credit account numbers
  - Personal financial information (e.g. financial aid data)
  - Account log-in credentials
  - Driver's license number or state-issued identification number
  - Health and medical records, including HIPAA-protected information
  - Export-controlled information
  - Human-subject research information
  - Other sensitive information that the information sponsor or responsible Vice President has determined must remain on a secure BC server.

**FAQ**

*Does this mean I can’t send any of the data in the new category via Google email, either?* The type of data in the new category (credit cards, etc) is not suitable for email. The restriction, however, is on off-campus data storage, not on email communications, so while sending such information in email is very strongly discouraged, it is not explicitly prohibited.

*What about H/R data or BC financial data?* These have not been declared by their Sponsors as falling into the new category at this time, so at this time they are allowed on Google Drive. If their Sponsors subsequently declare that this data falls into the new category, users of the data will be notified so they can take appropriate action, as outlined in the Data Security Policy under Sponsor and User responsibilities.
Do the above guidelines apply to personal accounts on Google? Only the BC version of Google Drive is approved for storing BC data of any type, not the consumer version of Google Drive. Obviously you can put BC “Public” information on a consumer account, but not other categories.

Doesn’t BC already store some of this type of information off-campus anyway? Exceptions can be made such that data falling into this new category can be stored off-campus if the service is vetted and approved by BC senior management. Any such exception must be requested and approved in writing. Until such time as the exception process is officially defined, please request any such exceptions by writing to “security@bc.edu”. Existing services the University has contracted for off-campus that have already undergone the required vetting will be receiving written exceptions.

Shouldn’t it be OK to store data in the cloud if it’s encrypted? Data in the new category that is encrypted before leaving BC in an approved fashion will also likely be exempted in the future. The fact that an outside “cloud” vendor encrypts will not be sufficient in and of itself to meet this future exemption. The list of approved BC encryption techniques is not available yet.

Is BC imposing this restriction because Google is less secure than some other storage location(s)? Google, Dropbox, and other general-purpose file storage services on the Internet are just that -- general file storage mechanisms. They simply were not developed to store regulated or classified data. These vendors, including Google, have refused in the past to sign agreements that they comply with some or all of the various regulations governing these types of data. This does not mean that the services aren’t secure for general use, it’s an acknowledgement that their target market is general use. We are confident that Google is a relatively secure service, or we would not be migrating the BC community to their service. BC’s stance outlined here may change over time as the vendors change, offer different services, or if BC develops or buys additional technology to protect data via encryption, etc.

Think of it this way -- we have recommended for years now that particularly confidential data not be stored on your local computer, but in the BC data center, not because your local computer is insecure, but because it’s not secured the same way as the data center. Based on “cloud services” reluctance to sign agreements saying that, for example, their “cloud drives” follow all the credit card protection regulations, we do not want BC users putting credit cards on them. This doesn’t mean there is a security problem with the services, just that they’re not secure enough for credit cards. Security is a continuum, not an absolute.