Terms of Service for UD Google Apps
rev. 9/1/12

The University of Dayton issues Google Apps accounts to all students, faculty, and staff. Google Apps is a popular communications and collaboration suite consisting of a core set of applications: Gmail, Calendar, Contacts, Docs/Drive, Sites, and Talk. The University has negotiated a unique contract with Google to safeguard the privacy and security of our data and community when using these core applications. The UD Google Apps account is the primary communication and collaboration tool used to conduct University business. (Note: UDRI is the only exception, as it uses a separate email system configured to meet specific requirements required due to government contracts.)

In addition, there are dozens of non-core Google services that can be accessed using a Google Apps account. In order for the University to introduce any of these non-core services, all UD Google Apps users must individually accept Google's generic Terms of Service agreement, which apply only to the non-core services. Core services remain protected by our Google contract. Even if you never intend to use any of these non-core services, you need to accept (acknowledge) the terms of use by which they are administered. Until you do this, access to your UD Google Apps account will be deferred.

The University of Dayton reserves the right, at any time and at its sole discretion, to add or remove applications and to modify the provisions of the UD Google Apps service and these Terms of Service. The information provided below explains the appropriate use of private and sensitive data as it relates to your role at the University. Use of UD Google Apps implies you have read, understand and agree to adhere to these Terms of Service and all other applicable guidance.

Appropriate Use of Private and Sensitive Data

You may use UD Google Apps, whether for personal business or to conduct University activities that are aligned with your role at the University, provided that you do so according to the University's Fair, Responsible and Acceptable Use Policy, and according to the restrictions for certain types of data as outlined in the University's Electronic Use of Confidential Data Policy.

Email, by its nature, is an unsecure medium for sharing sensitive information. Similarly, online data storage solutions (or "cloud storage") are only as secure as the rights you assign to your data. Before using any cloud storage solution (e.g., Google Docs, Dropbox) in the conduct of University business, you should make sure it's an approved solution and that you understand how to correctly assign and limit access to documents you upload.

Specific Confidential Data Concerns

Family Educational Rights and Privacy Act (FERPA) Data

FERPA is a federal law that protects the privacy of student education records. As a U.S. company, Google complies with all US laws including FERPA. UD specifically designated Google as a "school official" in its contract which means that Google may receive education records in order to provide this service without violating FERPA.

Faculty and Staff should still consider the end recipient in making determinations about FERPA compliance, but can confidently use UD Google Apps as an appropriate medium to share a student's education records with the individual student as well others as allowed by FERPA. For any specific FERPA questions, please contact the Registrar or Legal Affairs.

Health Insurance Portability Accountability Act (HIPAA) and Protected Health Information (PHI) Data

HIPAA is a federal law that protects the security and privacy of individuals' health data. UD Google Apps should not be used to store or transmit protected health information (PHI).

Intellectual Property Rights and Participation of External Users

Cloud based solutions such as Google Apps enable users to invite others, both internal and external to UD, to collaborate on data and documents. While this is a powerful new tool, it is the responsibility of the individual user to ensure appropriate sharing controls are assigned in order to protect intellectual property placed in cloud storage solutions and to prevent accidental or undesirable sharing of information.

Users should not use UD Google Apps for communications and/or work related to UDRI research.

Payment Card Industry (PCI) Data

The Payment Card Industry Security Council dictates how credit and debit card information must be handled. UD Google Apps should not be used to store or transmit protected credit and debit card information. View the University's PCI General Policy, which governs credit and debit card use.

Export Control Restrictions

The federal government restricts the sharing of certain goods, services and technologies with foreign nations and their agents. UD Google Apps should not be used to store or transmit anything falling into this category. Questions may be directed to UDRI's Office of Contracts and Grants Administration, 937-229-2919.

Recommendations for Use of Online "Cloud" Applications

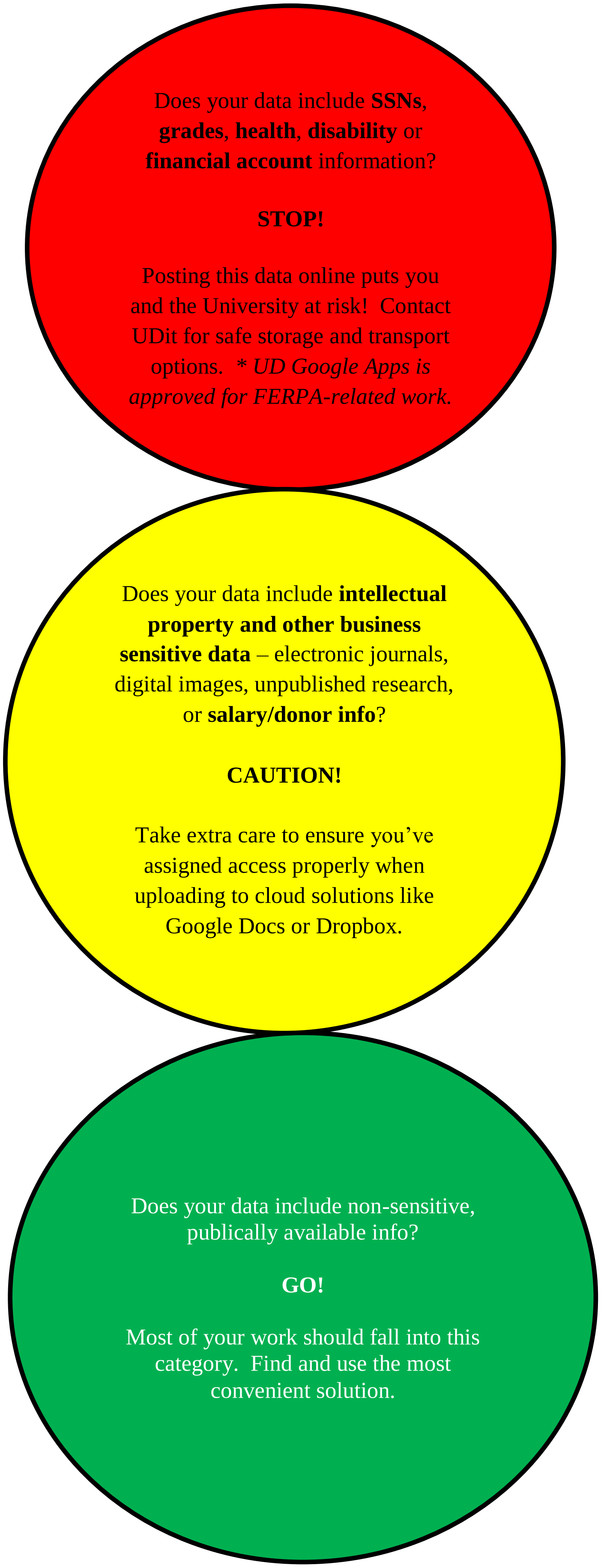
If you chose to employ online cloud solutions (Google Docs, Dropbox, etc.) for University-related documents, be aware that permissions on these applications must be carefully managed to prevent inadvertent "over-sharing". To protect the University, its constituents and yourself, make sure you follow these guidelines:

- Use a strong password and don't share it.
- Check the data contained within your documents to ensure no personally identifying information is present (e.g. Social Security numbers, grades, health, disability or financial data). Unless specifically approved, personally identifying information should never be uploaded to an online file storage system external to campus.

- Check the data contained within your document for any business sensitive information (e.g. intellectual property like electronic journals, digital images, unpublished research or salary/donor info). Business sensitive data must be stored carefully when using online file storage systems.
- Make sure you understand how access permissions are set within your file storage system. Google Docs, for instance, allows you to grant access to a single document or to a collection/folder/directory of documents. Be sure you don't "overshare" files to a larger audience than intended!
- Report incidents of compromise or any concerns to the appropriate personnel as outlined in the University's IT Incident Handling Policy.
- Contact the IT Risk Management Office (937-229-4387, itriskmgmt@udayton.edu) if you are not sure if your data is sensitive or would like more information regarding storage options.

Look Both Ways before Posting Data Online

Before you post files online, check the light for data safety!



Does your data include **SSNs**, **grades**, **health**, **disability** or **financial account** information?

STOP!

Posting this data online puts you and the University at risk! Contact UDit for safe storage and transport options. ** UD Google Apps is approved for FERPA-related work.*

Does your data include **intellectual property and other business sensitive data** – electronic journals, digital images, unpublished research, or **salary/donor info**?

CAUTION!

Take extra care to ensure you’ve assigned access properly when uploading to cloud solutions like Google Docs or Dropbox.

Does your data include non-sensitive, publically available info?

GO!

Most of your work should fall into this category. Find and use the most convenient solution.