LionMail Drive Requirements

Overview

One of the many features of LionMail is Google Drive ("LionMail Drive"), a cloud storage environment that houses documents and enables collaboration. The document outlines the security, accessibility and academic use requirements for LionMail Drive at Columbia University.

As a service managed by Columbia, LionMail is subject to the same security policies and oversight as other IT services managed by the University. Columbia's contract with Google provides protections that improve upon those in the consumer Google Apps license. For more information about LionMail and security, go to: http://cuit.columbia.edu/lionmail/lionmail-faq#security-faq.

LionMail Drive is currently available to the Columbia University community through LionMail. Please note, however, that faculty may **not** make the use of LionMail Drive mandatory in their academic interactions because it is not readily accessible to all students and requiring its use might exclude some students from full class participation and access to the full academic environment.
While Google continues to refine Drive to ensure full compliance with the Americans with Disabilities Act, and make sure it is accessible so that all individuals can use its features, students cannot be required to use LionMail Drive until full compliance is achieved.

Security

Use LionMail Instead of Consumer Google Apps

The University requires that Columbia students, faculty and staff who have access to LionMail Drive (and other LionMail apps) use LionMail in lieu of consumer Google Apps for University business, subject to the following limitations and recommendations. Any use of data by members of the University community will be subject to the following policies: Data Security Classification, Registration and Protection of Systems, Email Usage and Registration and Protection of Endpoints. For additional information, see the Administrative Policy Library.

Protect Data When Collaborating using LionMail Drive

All information should be protected from unauthorized access or unauthorized modification. Sensitive information, including the types listed below, should not be stored unencrypted on LionMail Drive.

1. **Protected Health Information** ("PHI,") covered by HIPAA, is sensitive patient information that is processed, transmitted or stored by organizations within the University that are subject to HIPAA regulations ("the Covered Entity"), as defined by the Office of General Counsel. For example, Columbia University Medical Center is defined by the Office of General Counsel to be part of the Covered Entity and therefore subject to HIPAA regulations.

   Patient information is considered PHI if it relates to the health status, clinical research or payment for health care and can be linked to an individual patient. For more information, view the University's Data Classification Policy. **Important: You cannot store PHI on LionMail Drive nor in any consumer service (e.g., GMail, Dropbox, etc.) at any time.**

   Please Note: The term PHI should not be confused with your own personal health information (e.g. your blood work or cholesterol test results).

2. **Personally Identifiable Information** ("PII") is sensitive information, such as Social Security numbers (SSNs), account or credit card numbers or driver's license numbers. For a complete list, view the University's Data Classification Policy. Unencrypted PII should never be stored in an email message or LionMail Drive ("Google Drive") Document, Sheet or Presentation. If you need to store or email PII, this information must be encrypted. To learn more, view the University's Encryption Policy.

   Credit Card Numbers. Credit card numbers or any other Payment Card Industry (PCI) data can never be stored or sent using any University system, including LionMail. Credit card numbers also cannot be stored using any consumer services (e.g., Gmail, Dropbox, etc.). To learn more, view the University's Credit Card Acceptance and Processing Policy.

In support of the Data Classification Policy, the University will utilize an automated system that identifies documents stored on LionMail Drive for unencrypted patterns that may resemble sensitive data, such as SSNs or credit card numbers. If such patterns are detected, sharing of the document to anyone not on LionMail will be automatically disabled and the owner will be immediately notified and given instructions on how to proceed.

Required LionMail Drive Sharing Settings

LionMail Drive offers sophisticated sharing capabilities that facilitate collaboration, but it is important that LionMail users are protected.

Approved Document Sharing

To share a Google document, use the setting:
"Private – Only the people listed below can access."

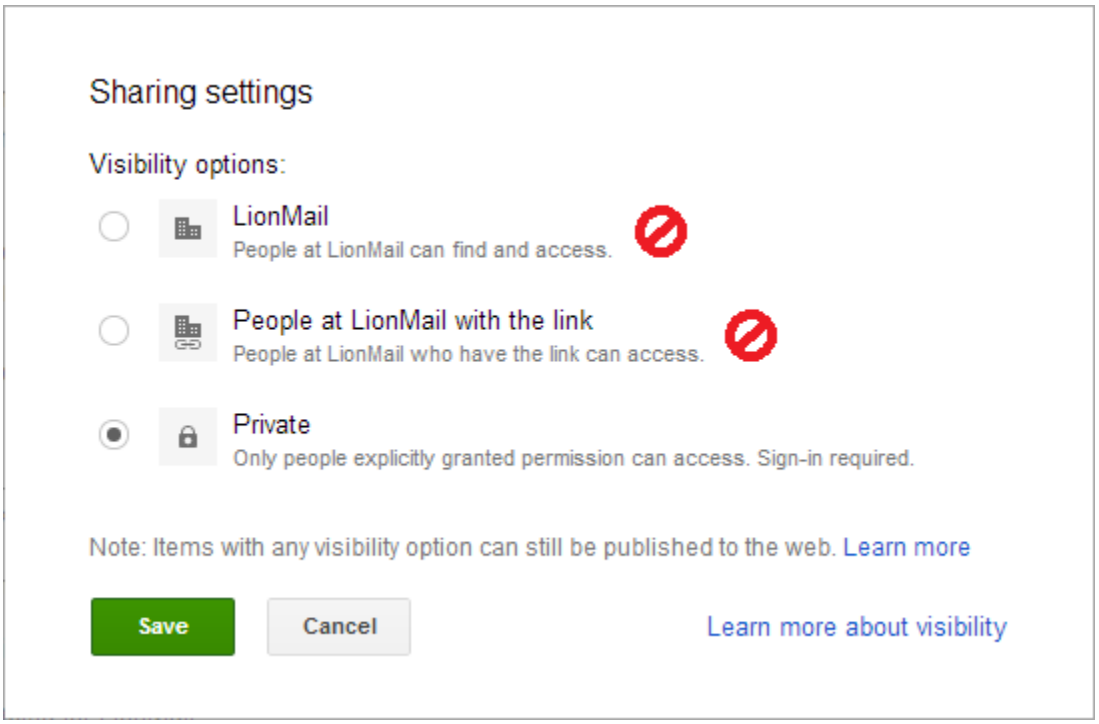
Then, add users. This level of sharing on LionMail Drive allows users to share a Google document with individual users.

Prohibited Sharing

To protect LionMail users, several LionMail Drive sharing settings are prohibited, including:

- "Public on the Web"
- "Anyone with the Link"
- "People at LionMail with the Link" – Documents with this level of sharing can easily be shared beyond your intended recipients
- "LionMail" – This level of sharing shares a document with *any* LionMail user, including students, faculty, staff, some alumni, and so on

The automated filtering system referenced above, will also filter Google documents for public sharing on LionMail Drive. If the system detects the public sharing of any LionMail Drive documents (such as, "Public on the Web"), sharing will be automatically disabled and a notification will be sent to the document owner.



Accessibility and Academic Use

Primary Guidelines

In compliance with federal, state and local laws, Columbia University is required to provide accessible programs and services. The University is committed to fostering a learning environment that is accessible for students with disabilities and therefore provides equal access to Columbia's programs and activities, including coursework and academic interactions. Faculty may **not** require students to use LionMail Drive or any of its features.

If a faculty member recommends the use of any LionMail Drive feature, he or she must:

- Post the following statement on the syllabus, course website or other course or programmatic materials:

Students with disabilities who are unable to access information from CourseWorks, the course website, LionMail Drive or other applications, must contact Disability Services at disability@columbia.edu to determine available accommodations, assistive technologies or alternatives. Students should contact Disability Services when they first encounter (same day) such difficulties to ensure timely resolution.

- Provide students with the link to Making Google Documents Accessible page: http://cuit.columbia.edu/google-drive-making-google-documents-accessible

- Require students to create accessible documents.

- Alert Disability Services by email (disability@columbia.edu) if a student with a disability reports having difficulty accessing electronic information or programs.

Additional LionMail Information

- LionMail and Security: http://cuit.columbia.edu/lionmail/lionmail-faq#security-faq
- Encrypting Sensitive Data: http://cuit.columbia.edu/cuit/it-security-resources/handling-personally-identifying-information/encryption-tools
- LionMail and Accessibility: http://cuit.columbia.edu/lionmail-drive-making-google-documents-accessible
- LionMail Drive Best Practices: http://cuit.columbia.edu/lionmail-drive