Instructions for Sharing Sensitive Information via Google Drive

We strongly encourage you to share documents with sensitive information using Google Drive. Sharing sensitive information directly in email is against College policy.

> ***You should only send via email using password protected files when it is the only option.*** *Sending via email, while the message is encrypted in transit, can sometimes cause misdirection (auto-fill) or errant forwarding of sensitive content. And frequently passwords used to "protect" files are easily guessable and weak - providing very little protection if the email were misdirected or received or accessible by the wrong person.*

When sharing information - ask yourself these 2 questions to determine how the information will be used and by whom. This will help you assign the least privileges that are needed and suggest the best ways to manage access to the information.

- ***Does this person or group need access?***
  This will help you identify if you can share the information and with how many people based on their need to know, role, or other criteria.
- ***What access do they need?***
  This will help you think about whether they need to modify or update the data you are sharing, whether those changes need to be managed or coordinated, whether they only need the data for a specific amount of time, and whether they should be able to share, copy, download, or print the data, etc.

Within the Amherst ecosystem (staff, faculty, trustees, students, volunteers, and alumni), share using Google Drive or Workday Drive. You have options to limit download, print and copy and you can even set expirations on the access. This also provides version control, collaboration, and transparency. The Amherst Google Workspace and Workday environments also require multi-factor authentication so you have more assurance that the person accessing the data is who they claim to be.

Google Drive now provides for visitor access as well - so you can share documents stored within the Amherst Google Drive with external parties who may not have a Google account. This provides the same or similar controls as those within the Amherst environment.

You can learn about visitor access at: https://support.google.com/drive/answer/9195194

When the external person/visitor gets the invitation to view the file you shared from Google Drive, they must verify their identity with a PIN. After that, they can collaborate on the shared file or folder for 7 days. If they need to access the file for longer, they can use the link from the original sharing email to verify their identity again.

Note: Visitors cannot own data within the Amherst Google Drive environment.