Security and Google Add-Ons for University Employees

Depending on how you use Google products, some of the information in your App State Google account may contain sensitive data. When you give access to third-party sites or applications, they may be able to read, edit, delete, or share this information.

Google products with especially sensitive information include:

- **Gmail:** Your University emails may contain sensitive or internal data including your contacts' names, your private correspondence, or an attached copy of a medical report.
- **Drive**: There may be sensitive data in Google Drive, like financial records, official reports, and presentations. In addition, if you've shared documents with other people, their names and contact information are also in your Google Drive.
- **Calendar:** Your Google Calendar can have important information about your daily routine and details about private events and appointments.
- **Contacts:** Your Google Contacts can include the names, phone numbers, addresses, and contact details of the people you know.

Consider the following before giving access:

- **How secure is this site or app?** If the third-party app's server is hacked, University data may be accessed by unauthorized people. When you allow third-party apps to access your App State Google Account, they can copy and save your data on their own servers. Google doesn't protect the data on another company's servers and your data may be subject to greater data security and privacy risks.
- **How will this site or app use my data?** The site or app may use the data in ways that are not obvious, such as being shared with others.
- **Can I delete my data from this site or app?** Depending on the app, you may be unable to quickly or automatically delete your data from their servers. It may also be difficult to delete the account you created on the app.
- **Who else can see my data on this site or app?** Some third-party apps or sites may have individuals who look at your Google account information, including emails you write, or your contacts.
- **What terms of service and privacy policies are applicable?** Most services utilize a Terms of Service and/or privacy agreement that must be accepted before use. The Office of General Counsel may need to help review these agreements before adoption and use.
- **Will this site or app tell me if something changes in their terms of service?** The site or app may not directly notify you if it changes its policies and practices.

How do I determine what add-ons I currently have?
Google gives you the ability to see what add-ons are attached to your account at: https://myaccount.google.com/permissions.

To Remove Access:
If you gave account access to a site or app you no longer trust, you can remove its access to your Google Account. The site or app won't be able to access any more info from your Google account, but you may need to request that they delete the data they already have.

1. Go to your Google Account.
2. In the top navigation panel, select "**Security**".
3. On the *"**Third-party apps with account access**" panel*, select "**Manage third-party access**".
4. Select the site or app you want to remove.
5. Select "**Remove Access**" then click "**OK**".

To Report a Site or App:
Go to the Apps with access to your account section of your Google Account (You might need to sign in.)

1. Select the app you want to report.
2. Choose "**Report this app**".

Related Knowledge Base Articles

- Notifications in Google Forms
- Google Calendar Appointment Slots

Search Knowledge Base

Submit a Service Request

We value your feedback! Click HERE to suggest updates to an existing article, request a new article, or submit an idea.