Security and Google Apps

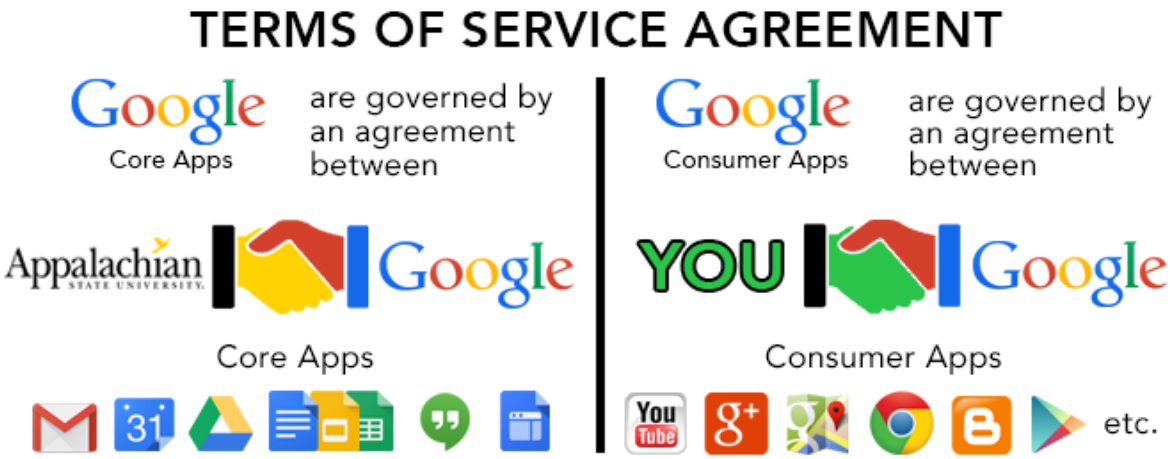
Google Apps at Appalachian State University, also known as "MountaineerApps," includes a wide range of services that can store and transmit information. App State has formed a contract with Google that helps protect the privacy and confidentiality of university students, faculty, staff, and alumni data stored in the Appalachian Google core apps suite of services (see question #2). In addition to this contract, our own utilization of MountaineerApps must take into account legal requirements and Appalachian State University policies.

1. Who owns the data stored in MountaineerApps?

As specified in our contract with Google, App State retains ownership of all institutional data stored in core MountaineerApps (see question #2).

2. What is the difference between Google Core Apps and Consumer Apps?

App State's agreement with Google covers a set of applications and services referred to as "Core Applications." In addition, Google also offers a range of consumer applications within our Google domain that can be enabled by the individual user. These consumer applications are governed by agreements between the end-user and Google. These applications are referred to as "Google Consumer Apps."



What to know about Core Applications

Our use of Core Applications has a number of contractual protections related to the Family Educational Rights and Privacy Act of 1972 (FERPA), intellectual property, confidentiality, and data security. Google has also made contractual commitments to omit advertisements from these services. These services are subject to University appropriate use guidelines and electronic records policies (see section #4 for more information).

The Core Apps include:

- MountaineerMail (Gmail)
- MountaineerCalendar (Google Calendar)
- MountaineerDrive (Google Drive)
- MountaineerContacts (Google Contacts)
- MountaineerHangouts (Google Hangouts)
- MountaineerSites (Google Sites)

What to know about Non-Core Applications

Google's Consumer Apps are governed by a contract between end-users and Google. If you would like to use Google's Consumer Apps with your MountaineerApps account, you will need to agree to Google's Terms of Service and Privacy Policy. Google's Consumer Apps, or "Non-core Apps," include all applications besides the Core Apps listed above, such as:

- YouTube

- Blogger
- Maps
- Translate
- Google+ and many more

Google Consumer Apps are not subject to the same protections that App State has in place for the Core Apps, and, most importantly, they are not FERPA compliant.

It's important to know that information stored in or transmitted via any Consumer App is subject to use by Google under the terms of agreement between the user and Google. Google Consumer Apps often contain specific terms of use regarding privacy, security, government access, and support. One Consumer App, Google+, requires all users to be at least 13 years of age so please enter your birthdate carefully. Never post confidential information in any Google Consumer App in order to avoid the risk of exposing sensitive information. We strongly encourage you to read the privacy terms and terms of service for any Google Consumer App prior to its use and think carefully about what you post on any social medium and the repercussions of it being made public.

3. Is data stored On MountaineerApps private?

Per our contract, Google agrees not to scan, access, or otherwise inspect content stored in MountaineerApps except for support purposes (i.e., blocking spam, scanning for viruses, facilitating search features).

App State is subject to the North Carolina Public Records Act (NCGS Chapter 132), which provides a method for third parties to request records associated with the public business of all state agencies, including App State. Information stored or transmitted through MountaineerApps may be subject to the North Carolina Public Records Act and require disclosure to third parties. Some information is exempt from these records requests (see Appalachian Public Records Requests Policy for more information).

***If you receive a public records request, please contact the Office of General Counsel before responding to this request**.

4. Is data stored within MountaineerApps secure?

As part of our review of Google Apps, ITS examined the security measures and obligations that Google extends to maintain the privacy and security of their customers' data. Google utilizes advanced security measures to protect Google Apps content which would be fiscally infeasible for App State to provide. While no system is completely invulnerable to security issues, the Google Apps platform is sufficiently secure to store, transmit, process, or manage most information that the University utilizes in the course of daily business.

However, it is important to be aware that some materials are not suited for utilization within Google Apps based on risks or legal requirements (please see item below).

- Google Compliance and Security WhitePaper

5. What data should not be used with MountaineerApps?

While Google Apps provides robust security, it is by its nature not appropriate for storing, transmitting, or managing certain types of confidential or restricted institutional data. The Office of Information Security has developed guidance on Secure Storage and Sharing, as well as a one-page on Data Classification Guidance. To be clear, the following data types should never be uploaded, stored, transmitted, or managed using MountaineerApps:

Personally Identifiable Information (NC Identity Theft Protection Act)

App State has legal obligations under state law (NCGS 75-60) to protect a wide range of personally identifiable information that may be entrusted to us. Google Mail, Google Drive, and other MountaineerApps by their nature are not appropriate mediums for storing or transmitting this type of information.

For this reason, the following data types should never be uploaded, stored, or transmitted using MountaineerApps:

- Social Security Numbers
- Drivers License Numbers
- State Identification Card Numbers
- Passport Numbers
- Biometric Information
- Account Passwords
- Digital Signatures

Confidential Financial Information (GLBA, PCI-DSS)

App State has both contractual and legal obligations to protect various types of confidential financial information.

The following financial data types should not be stored or transmitted using MountaineerApps:

- Credit Card Numbers
- Debit Card Numbers
- Check/Savings Account Numbers

Protected Health Information (HIPAA)

Individually identifiable protected health information (PHI) is legally protected by Federal Health Insurance Portability and Accountability Act's Privacy as well as North Carolina laws related to medical record confidentiality.

Protected health information should not be transmitted or stored using MountaineerApps. Instead, PHI should remain in University-approved record systems designed to contain health information and should be de-identified (stripped of all 18 HIPAA identifiers) before it is shared electronically. If de-identifying the information is not possible, then appropriate methods for securely transmitting the information include:

- Appalachian File-locker Services
- A secure "facsimile system," as defined by HIPAA

Additional obligations to remember when sharing PHI:

- Limit the amount of information to the minimum required.
- Immediately report misdirected PHI, or incidents involving the inappropriate use or disclosure of PHI. The misdirected PHI must be included in all reports.
- Ensure that the recipient of the information is legally authorized to receive the information.
- Before sending the email or sharing the document, verify the list of recipients of the email or others having access to the communication carefully in order to prevent inadvertent disclosure.

Export Controlled Information

The United States export control laws forbid the unlicensed transmission of controlled items, software, and information to certain countries. These export control laws apply to controlled items even when transmitted primarily for storage or for further transmission purposes. Users of MountaineerApps must be aware that their data may be stored in data centers outside the United States.

For these reasons, **researchers working with controlled material should use another, secure means of data transmission**. Export-controlled information is not permitted in MountaineerApps, including transmission via the Gmail service. If you are uncertain whether your data are subject to export control laws, and/or whether you can send this data via email, please contact the Office of Research Protection at 828-262-2692.

- Appalachian Office of Research Protection - Export Control Policies

6. How can I exchange confidential or sensitive data with authorized App State employees or third parties?

To facilitate the secure exchange of information, ITS has established a secure file exchange platform called Appalachian Filelocker. Appalachian Filelocker is a secure temporary file transfer application that can be used to easily encrypt and share data both within the University and with authorized third parties. More information on Filelocker can be found at the link below:

- ITS Fileshare

7. Can I use MountaineerApps to store FERPA-protected data?

The Family Educational Rights and Privacy Act of 1972 (FERPA) is a federal law that protects the privacy of student education records. Student data protected by FERPA is permitted in Core MountaineerApps when these records do not contain confidential data elements (see #5 above on what data not to use with MountaineerApps). FERPA-protected data is subject to access by school officials who have a legitimate educational interest as well as by other identified officials, as defined and identified by the university's FERPA policy.

To the extent that Google has access to student education records as a contractor for the University, it is deemed a "school official," as defined by FERPA, under our contract, and will comply with its obligations under FERPA. No University personally identifiable student data should ever be made publicly accessible without the student's signed consent.

For more information, see:

- Appalachian Policy Statement On The Family Educational Rights and Privacy Act
- Office of The Registrar - FERPA and Student Records Access

8. Intellectual property rights and participation of external users

MountaineerApps users can invite other Google Apps users, both within the university and outside the university, to view data, co-edit documents, and use other collaboration tools. It is the responsibility of each user to ensure that appropriate sharing controls are used in order to protect App State's intellectual property or third-party confidential proprietary information provided to the university under contractual terms requiring non-disclosure.

9. What constitutes acceptable use of core MountaineerApps?

The acceptable use of MountaineerApps is no different than other App State computing services and is covered under a number of Campus policies.

In general, the following activities are not acceptable uses of MountaineerApps:

- Send unwanted messages that may contain harassing or content that may reasonably be deemed as obscene.
- Damage or degrade system functionality including users' efficient utilization of Internet services.
- Gain unauthorized access to a system or data that you have not been given explicit authorization to use.

- Promoting/conducting business for personal use or engaging in political activity including sending bulk email messages.
- Copy, transmit, or disclose copyrighted data, software, or documentation without proper authorization.
- Disseminate confidential or sensitive data to unauthorized individuals.

More information on relevant University policies can be found here:

- Use of Computers and Data Communications
- Information Security Policy
- Statement of Confidentiality
- E-Mail As Official Means of Communication
- Political Activity and Public Officeholding

10. Can I utilize third-party applications with MountaineerApps?

Yes. There are numerous third-party applications that are capable of expanding the functionality of MountaineerApps in valuable ways. However, because each of these services has its own terms of service and varying degrees of access to read or modify university data, these third-party applications must be reviewed to ensure that their utilization is consistent with university legal, compliance, and risk objectives. To request a review of a third-party application, extension, or additional Google app, **submit a support ticket and choose MountaineerApps as the incident type, and Request New App or Extension as the Issue type and request a review.**