How to Google @ UNIVERSITY of ALASKA SOUTHEAST

G Suite for Education includes cloud-based services available to all members of the UAS community. G Suite for Education includes privacy provisions not found in its commercial products making it more suitable for educational use (see: https://edu.google.com/trust). Properly used, the G Suite provides collaboration tools with security controls adequate for protecting the University's public and internal-use data. The purpose of this document is to provide guidance on how G Suite should be safely used at UAS.

Points to keep in mind:

- Google's strength is in personal sharing and collaboration. It is not as strong at securing institutional/department records, especially in the long-term.
- Google provides features to enhance security, but these are not well known and can require IT assistance to set up.
- The suitability of Google for an application depends on the current Google contract language.

Key questions when considering the use of Google (G Suite):

1. **Is there a need to control the retention of materials (data, documents, etc.)?**
   A lack of retention control may result in records being unexpectedly lost or unintentionally retained longer than they should. Retention control is especially important for some internal-use document or FERPA protected records.
2. **What kinds of documents/records/data are involved?**
   UA data classification standards are found in UA regulation R02.07.094. Additional information is on the UA Records and Information Management website (https://www.alaska.edu/records/dataclass). University regulation provides three classifications:

	PUBLIC	INTERNAL USE	RESTRICTED
Legal Requirements	Data approved for general access by appropriate UA authority.	UA has best practice (due care) reasons to protect data.	Protection of data is required by law or best practices.
Risk Level	**Low**	**Medium**	**High**
Examples	Press statements; brochures; job titles/descriptions	Internal committee documents; public research; supporting documentation for business functions	Educational records; medical records; counseling notes; protected research; credit card/banking numbers; SSNs
Guidance	Records classified as **public** can be placed and freely shared in G Suite.	**Internal-use** records can be placed in G Suite; however, records should either not be shared, or should only be shared with managed groups.	Most **restricted records** should not be placed in the Google environment. There are exceptions. FERPA protected data can be in Google; however, precautions must be taken.

adapted from R02.07.094

- It is strongly recommended that staff consult with IT prior to using G Suite for **restricted** data.
- In all cases, the need to control the retention of records may require different approaches to how G Suite is used.

updated: 6/8/2017

Google Guidance

	Retention control not a concern	Retention control needed
PUBLIC DATA	**#1 Normal Google Use** Keep private or share as needed • Draft public documents • Press statements • Agenda or minutes for public meetings	**#2 Institutional Ownership** Change owner to UAS.Docs@alaska.edu • Campus promotional material • Final versions of documents • Non-confidential forms & data
INTERNAL USE DATA **SOME RESTRICTED DATA**	**#3 Managed group sharing** Share only with managed groups • Draft non-public documents • Short-term work-team documents • Individual professional notes	**#4 Google "Fileshare"** Institutionally "owned", managed access • Forms/data supporting department processes • Departmental records • Committee work, minutes, etc.
MOST RESTRICTED DATA	**Not suitable for Google** Use alternative tools (seek guidance as needed) • HIPAA data (ex: health records, counseling records) • PCI/Financial data (ex: credit card info, banking numbers) • Protected personal information (ex: SSNs) • Sensitive/protected research	

#1 Normal Google Use

For public data with no retention concerns, documents can be created, retained or shared with others (both internally or externally) without concern.

#2 Institutional Ownership

Most Google documents are "owned" by the user who initially created them. Since records are purged when personal Google accounts come and go, and it is important to change the owner from an individual to an institutional account in order to retain control over document retention. The institutional account UAS.Docs@alaska.edu exists to ensure records can be retained as individuals come and go.

#3 Managed Group Sharing

Employees may retain their access to Google long after they are terminated from the University. This means that they will continue to have access to any internal-use or restricted records which have been shared with their personal Google accounts.

For non-public records, it is important to either not share the documents, or to only share with managed groups. A managed group is one which is either maintained automatically by IT, or which is actively managed by department staff. Many managed groups exist already. Example of current groups include: current faculty and at each campus, specific departments such as IT or Admin Services, and various committees and work-teams. IT can assist with creating new groups as needed.

#4 Google "Fileshare"

This is the most secure strategy for storing records in Google. A Google "Fileshare" is very much like a traditional windows departmental fileshare. It combines the functions of institutional ownership (#2) with Managed Group Sharing (#3). Document placed in a "Google Fileshare" folder will automatically become owned by the fileshare account and access is controlled by an associated managed group. Contact the IT helpdesk to request the setup of Google fileshares.