Williams College Cloud Storage Security Policy

Data owned, used, created or maintained by the College is classified into the following three categories:

- Legally protected
- Need to know
- Public

The [Williams College Confidentiality Policy](#) describes these categories in more detail.

‘Legally protected information’ includes personal information (social security numbers, bank account numbers, credit card numbers, driver license numbers), FERPA protected information, financial information that is not public (protected by Gramm-Leach-Bliley Act), and personal health information (protected by HIPAA).

‘Need to know’ information includes employee information such as salary data, evaluation data, biographical information etc., faculty research projects related information, student financial data, academic information etc., alumni information such as gift and pledge data, home addresses, phone numbers etc., and nonpublic financial information of the College.

‘Public’ information is information that may be released to the public without the person’s consent.

What is Williams College Google Drive?

Williams College Google Apps are a set of services provided by the Office for Information Technology that give people at Williams College access to Google’s features and tools, but with additional special protections and provisions not available with the consumer version of Google services.

Williams College Google Drive is a [cloud-based file storage service](#) provided by Google under this special contract.

Using Williams College Google Drive has several benefits:

Updated 4/2/2014
1. It lets you store and access your files anywhere – on the web, on your hard drive, or on the go. Change a file on the web, computer, or mobile device and the updated version is available on every device where you’ve installed Google Drive.

2. Any time your device has Internet access, it checks in with Google Drive. Your files are automatically synchronized and kept up-to-date.

3. This service makes the secure sharing and collaboration much easier:

   - Google Drive lets you choose exactly who has access to your files with easy-to-use access controls. You can share just the one specific document or file with someone, or set up a folder in Google Drive so that specific people have access to an entire folder. How granular you get is up to you. That said, we recommend making security easy to maintain by keeping the permissions you set up simple, set up a folder for each different group/community with whom you want to share documents.

   - Assuming your permissions are set up correctly, your files are safer; you don’t need to email attachments anymore.

If you choose to use Williams College Google Drive, you are personally responsible for setting up security correctly. If you have questions, contact the Office for Information Technology.

Approved for Williams College Cloud Storage

<table>
<thead>
<tr>
<th>Category</th>
<th>Type of Data</th>
<th>Special Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legally protected</td>
<td>Personal Information</td>
<td>Must be password protected</td>
</tr>
<tr>
<td>Legally protected</td>
<td>Financial Information that is not public (Gramm-Leach-Bliley Act)</td>
<td>Must be password protected</td>
</tr>
<tr>
<td>Legally protected</td>
<td>FERPA information</td>
<td></td>
</tr>
<tr>
<td>Need to know</td>
<td>Salary information</td>
<td>Must be password protected</td>
</tr>
<tr>
<td>Need to Know</td>
<td>Evaluation information</td>
<td>Must be password protected</td>
</tr>
<tr>
<td>Need to Know</td>
<td>Faculty research information</td>
<td>Must be password protected</td>
</tr>
<tr>
<td>Need to know</td>
<td>Gift &amp; pledge information</td>
<td>Must be password protected</td>
</tr>
<tr>
<td>Need to know</td>
<td>Home addresses, phone numbers</td>
<td></td>
</tr>
<tr>
<td>Need to know</td>
<td>Nonpublic college financial information</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>Information that can be released without consent</td>
<td></td>
</tr>
</tbody>
</table>

Updated 4/2/2014
*** If you are going to store general work related files in the cloud, we recommend that you use the Williams College version of Google Apps (as opposed to the consumer version). The Williams College version includes privacy and security features not available in the consumer version.

**NOT Approved for Williams College Cloud Storage**

<table>
<thead>
<tr>
<th>Category</th>
<th>Type of Data</th>
<th>Special Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legally Protected</td>
<td>HIPAA</td>
<td>Should <strong>never</strong> be stored on Drive</td>
</tr>
</tbody>
</table>

All Williams College faculty and staff are expected to be familiar with the following policies that explain how to handle information properly.

- Williams College Information Security Plan  
  [http://oit.williams.edu/policies/information-security-plan/](http://oit.williams.edu/policies/information-security-plan/)

- Computing Ethics and Responsibilities guide  
  [http://oit.williams.edu/policies/ethics/](http://oit.williams.edu/policies/ethics/)

- Privacy Policy  
  [http://oit.williams.edu/policies/privacy/](http://oit.williams.edu/policies/privacy/)

- Williams FERPA Guidelines  
  [http://web.williams.edu/admin/registrar/facsis/ferpa.html](http://web.williams.edu/admin/registrar/facsis/ferpa.html)

- Williams College Confidentiality Policy  
  [http://wiki.williams.edu/display/handbooks/Confidentiality](http://wiki.williams.edu/display/handbooks/Confidentiality)

**Important**

Failure to comply with the standards put forth in this policy may result in harm to individuals, organizations or Williams College. The unauthorized or unacceptable use of College Data, including the failure to comply with these standards, constitutes a violation of College policy and may subject the User to revocation of the privilege to use College Data or Information Technology or disciplinary action.

Updated 4/2/2014