# Actions Required by the Google Workspace for Education Administrator

This document explains all steps needed to integrate the KGS Website with the existing Google Workspace for Education account.

## 1. Enable Required APIs in the Domain

The website requires access to multiple Google APIs. The Admin must ensure these APIs are allowed for domain accounts:

* Google Drive API
* Google Docs API
* Google Sheets API
* Google Slides API
* Google Calendar API

### ****Steps:****

* Go to Admin Console → Security → API Controls → Enable these services.
* Make sure all domain accounts are allowed to use these APIs.

## 2. Grant Domain-wide Delegation to the Service Account

The website uses a service account to manage file uploads and edits programmatically.

### ****Service Account Details:****

* Email: kgs-web-service-account@kgs-web-project.iam.gserviceaccount.com
* Unique ID: 118348104168435635958

### ****Steps:****

* Go to Admin Console → Security → API Controls → Domain-wide Delegation.
* Add a new client:
  + Client ID: 118348104168435635958

### ****Scopes:****

* + https://www.googleapis.com/auth/drive
  + https://www.googleapis.com/auth/drive.readonly
  + https://www.googleapis.com/auth/drive.file
  + https://www.googleapis.com/auth/documents.readonly
  + https://www.googleapis.com/auth/spreadsheets.readonly
  + https://www.googleapis.com/auth/presentations.readonly
  + https://www.googleapis.com/auth/calendar.readonly

This authorizes the service account to impersonate users in the domain, allowing the website to operate on behalf of approved staff members.

## 3. Create a Shared Drive for website Content

The upload feature of the website requires full edit control over a shared drive to store content.

### ****Steps:****

1. Create a new Shared Drive (KgsWebDrive).
2. Add the service account as a Manager (or Content Manager).

* This allows the website to upload, edit, and organize files automatically.

### ****Public viewing:****

* Set the drive or relevant folders to Anyone with the link → Viewer.
* This allows website visitors to view/download files while restricting uploads to staff only.

## 4. Create a Google Group for Upload Permissions

The website’s secure upload feature ensures that only authenticated staff members can upload files.

### ****Steps:****

1. Create a Google Group (example: website-uploaders@kellgradeschool.com).
2. Add all teacher/staff accounts that should be allowed to upload via the website.
3. Share the Shared Drive with the group as Content Manager or Manager.

* This gives group members upload/edit access while keeping public viewing restricted.

## 5. OAuth 2.0 Client ID Approval

Website may allow staff to log in with Google accounts, so Admin needs to approve the OAuth client.

### ****OAuth Client Details:****

* Name: kgs-web-client-1
* ID: 1059949445564-1m8kntn97922osoa89ipev2ofm107dr7.apps.googleusercontent.com

### ****Steps:****

1. Go to Admin Console → Security → API Controls → Manage Third-Party App Access.
2. Whitelist the OAuth client and approve it for the same scopes listed above.

## Summary of Permissions

|  |  |  |
| --- | --- | --- |
| **Entity** | **Role** | **Access** |
| Service account | Manager | Full upload, edit, organize |
| Staff Google Group | Content Manager | Can upload files via plugin |
| Public / Anyone with link | Viewer | Can view/download files only |

This ensures that:

* Only approved staff can upload files through the website.
* Public users can view/download shared content.
* The website can manage files via the service account securely.