Introduction to managing Google's G Suite and working in the cloud

This guide introduces some of the considerations schools typically have to give around working differently in the cloud environment, particularly when it comes to using Google's G Suite (previously known as 'Google Apps').

The guide is intended for technicians and teachers or support staff that have responsibility for managing and leading digital technologies in schools that use G Suite. It is most suited to small and medium sized schools that do not have in-depth, specialist technical support provision.

Contents

Once you have read this guide you are welcome to contact the Connected Learning Advisory to get more personal assistance. We aim to provide consistent, unbiased advice

and are free of charge to all state and state-integrated New Zealand schools and kura. Our advisors can help with all aspects outlined in this guide as well as provide peer review of the decisions you reach before you take your next steps.

For more information visit www.connectedlearning.org.nz
Check out our resources at resources.connectedlearning.org.nz
Call us for personalised service on 0800 700 400
Make a personal inquiry via our online form at query.connectedlearning.org.nz
Email info@connectedlearning.org.nz

Getting Started	G Suite for Education (previously known as Google Apps for Education) is free to state and state-integrated schools. Please see our Guide to Setting up Google's G Suite for Education for your School or contact the Connected Learning Advisory If you need assistance to get your system set-up.
	Training
	Consider how you can access training for being an administrator for G Suite. This is typically found online or delivered by professional learning or technical providers. If possible, ensure more than one person is trained and is actively being an administrator as this is part of good succession planning.
	Parental Permissions
	You should seek the permission of parents or caregivers before setting up their children's accounts. This VLN discussion may help with suggestions on how to communicate with parents about providing accounts.
	Sources of Help
	There are a variety of sources of help with administration in a cloud-based systems. Reaching out to connect with others is one of the best ways to learn.
	G Suite Administrator Help Centre
	Virtual Learning Network
	Google Educators Group - New Zealand
	Domain Best Practices - Google's own education-specific guide to setting-up G Suite

User Accounts

Adding Users

Adding users, like students, teachers and support staff, to the directory is usually done manually by an administrator or automated by a scripted process. Ideally your user accounts should be provisioned automatically with your Student Management System (SMS) being the authoritative source of users coming and going. Some SMSs allow for this to happen by feeding data to the school's network directory which can then synchronise the user accounts with the cloud system's own directory.

Whether automated or not, having robust procedures for setting up and managing user accounts in a timely fashion is essential for students and teachers to be able to use the cloud services that are available.
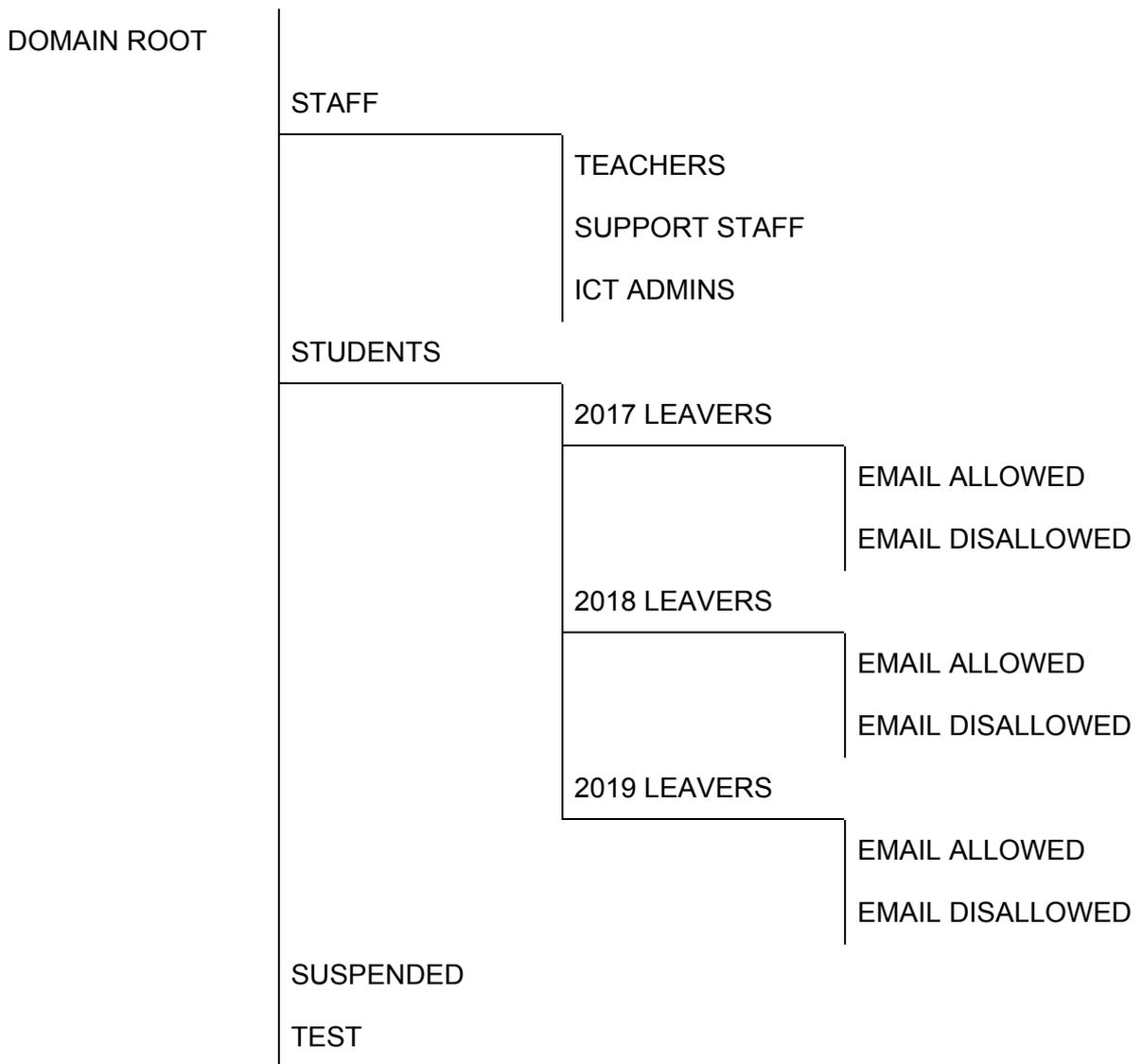
Multiple Users

There are two key ways that multiple users are identified and managed in bulk: Organisational Units (OU's) and Groups. Organisational Units are distinctly separate in their function to Groups, as explained below.

Organisational Units

Organisational Units separate the allocation of things such as the services, settings, policies and apps that are allowed or deployed to users.

Usually schools separate Staff and Student users as a minimum at the top level of OUs. Then, the OU structure could be further granulated, depending on the specific needs around which types of user require different services, settings, policies and apps. By separating students into OU's using the year in which they leave the school (as opposed to their current year level), students can remain in that OU rather than an administrator having to rename it each year:

```
DOMAIN ROOT

    STAFF

                    TEACHERS

                    SUPPORT STAFF

                    ICT ADMINS

    STUDENTS

                    2017 LEAVERS

                                    EMAIL ALLOWED

                                    EMAIL DISALLOWED

                    2018 LEAVERS

                                    EMAIL ALLOWED

                                    EMAIL DISALLOWED

                    2019 LEAVERS

                                    EMAIL ALLOWED

                                    EMAIL DISALLOWED

    SUSPENDED

    TEST
```

	Some tips:
	● Ensure users are assigned to the correct groups when their accounts are created.
	● Train your office/administration staff to be able to create and manage users and groups.
	● Ensure you have documented procedures for creating and maintaining user accounts.

Groups

Putting users into groups makes it easier to assign the access permissions for things like files, folders, calendars, email distribution lists, etc.

Naming groups with a prefix such as GRP- or an underscore ' _ ' makes it easy to see at a glance that it is a group rather than an individual e.g: _AllTeachers, or GRP-Teachers. Use a naming convention that is easy to follow rather than written in code.

Some typical groups might be:

> _AllStaff
>
> _AllTeachers
>
> _JuniorSyndicate
>
> _ScienceDept
>
> _StudentsYr9

Groups can be created and managed separately in the admin console or they can be synchronised with the groups that are already in place on the school's network directory. Whatever system is used, it is essential to have clear systems, roles and responsibilities around maintaining group memberships. It does not require technical expertise to administer group membership so designating this task to administration staff is recommended. However, it's important to provide sufficient training and ensuring that the tasks can be done by more than one person as this is good succession planning.

Some SMS providers enable groups to be exported automatically. This can be an effective system to enable the Groups in the cloud system to match the year levels, classes, subjects etc. that the students and staff belong to.

What to do when people leave the school

When an account is deleted, any files, folders, emails, calendars etc that that person has created are also deleted so it is important to consider what content needs to be retained by the school, what needs to be downloaded or transferred to that person and what should be archived.

Rather than deleting accounts, they can be suspended which means that the shared content is still accessible to others but the

user themselves can not log-on to retrieve it. Alternatively, when a person leaves the school, ownership of their files can be transferred to another account such as a generic 'past users' account or to a particular person.

Another option to consider is to rename the user who is leaving to 'deleted_$Name', change the password and disable email for that the account.

Our draft guide What to do with Google Accounts and Data when Students and Teachers leave your school provides much greater detail.

Setting up a Shared Folder Structure

Setting up a good filing system (folder structure) for storing and sharing files is important.

You may find that the folder structure you were already using on your server is suitable and you would simply like to duplicate this into your cloud service, or you might decide that this is time for a change.

With any filing system, it is always useful to have clear naming protocols for files and folders that are understood and used by anyone with access to it. If you have named a file/folder carefully in your cloud service, the search function will quickly locate it.

Thinking about who needs access to which files and folders is important. Best practice from a security perspective is to limit access to files and folders to only those who really need it.

Setting up a folder structure for shared folders requires some planning. Once the shared folder structure has been created, the groups that are to use the folders can be assigned suitable access permissions. The top two or three levels of the shared folder structure should be owned by a generic service account (eg: folders@abc.school.nz) and shared so that they are 'view only' otherwise people will likely add files and folders that turn the orderly structure into chaos!

Once the structures and permissions are in place, people will need to locate the top level shared folder in their 'Shared with me' folder and 'Add to my Drive'.

We also recommend you look at [Team Drives on the G Suite Learning Centre](#) for suggestions on how to use [Team Drives](#) to create a shared folder structure.

You might also be interested in:

- [A department folder structure in a New Zealand high school](#). Note that the grey folders are staff access only and the purple folders are also shared with students.

- Pressing 'SHIFT + Z' from within Google Drive to add files and folders to more than one folder at a time. This can be useful for teachers who want to have their own personal folder structure as well as use the centralised system.

Expectations of sharing resources

It's a good idea to establish clear expectations (possibly through a policy) around the sharing of resources in your cloud service. You might consider:

- What files/resources must be filed in the shared file system?

- What files/resources should not be stored on the school Drive or Sharepoint Site.

- Do teachers have to share all resources they create?

- Where will the files be stored? (i.e. "everything in its place")

- What types of files/resources are allowed to be shared outside of the school domain?

- Naming conventions

There are admin console settings available for [sharing outside of the school domain](#).

This may be a good opportunity to consider your school's policy around who owns the resources a teacher produces, and whether you want a [Creative Commons policy in place](#).

How to avoid files and folders from being deleted

When giving others editing rights to files and folders it is possible for items to be deleted. Options for minimising accidental deletion of files include:

- Establish the clear expectation that files are not to be deleted or removed from shared folders except by identified people/roles.

- Make certain files/folders 'view only' to those with whom they are shared.

- Backing-up files stored in cloud services is recommended for at least the most important users. The [G Suite Marketplace](#) lists back-up solutions. Having a separate back-up will also enable Drive files to be restored if a ransomware attack leads to files, other than native G Suite files like Docs or Sheets, being encrypted hence inaccessible.

Email Attachments - Sharing versus Sending

Once a folder structure and groups have been put in place, people can start to benefit from being able to more easily create and share files and folders. Sharing files and folders means that everybody is always accessing the latest version and they can collaborate on one document from different locations at the same time. For this reason always encourage people to share files rather than send attachments.

Managing Multiple Cloud Accounts, Identities and Passwords

As everybody gets more online accounts, be they from school-related activities or personal accounts, it is easy to be confused about which account is being used at any one time and to manage many different usernames and passwords.

Personal and School On-line Activities
It is best if personal and school-related online activities are kept separate. Some ways to do this include:

- Ensuring that you have personal and school accounts for different services such as Facebook, Twitter, Email, Photos, Documents etc.
- Using separate school and personal identities when online and keeping personal and school related browsing activities separate.

Passwords
According to the Verizon 2016 Data Breach Investigations Report, 63% of confirmed data breaches involved weak, default or stolen passwords.

We recommend that your strategy for password security should be centred around both highly secure and highly useable practices. This will increase security with little impact on staff. We recommend that you consider using:

- 2 factor authentication where possible to better prove your identity. See Add 2-step verification.
- single sign on for those services that allow it
- a password manager so you can manage having different passwords for different accounts
- long phrases as a password - length is more important than complexity

See the CLA's Recommendations for managing passwords for more information.

Shared Calendars

Setting up shared calendars can help everybody know what is going on at school.

People or groups of people can contribute to particular calendars so that the responsibilities for maintaining calendars are more effectively shared which leads to more reliable, up to date calendar entries.

Some tips include:

- Set-up separate shared calendars for different purposes. Then overlay them all for an overview of everything happening at the school. For example, Takapuna

[Grammar School's public calendar](#) comprises a series of calendars that the viewer can toggle on or off:

- Use Groups to give suitable permissions to just view or to edit calendars.
- Make sure that the default calendar sharing is only free/busy information otherwise everybody in your school will be able to view each other's appointments.
- Use shared calendars for booking resources such as rooms, vehicles or other items.

For more information about setting up shared resource calendars see [About Calendar Resources](#).

This guide has been produced in response to a number of specific queries about managing G Suite from schools.

It should not be read as a recommendation or endorsement of any specific product. The Connected Learning Advisory is a Ministry of Education supported service that provides schools with technology information relevant to their queries and does not recommend one product over another.

Date Last Updated: 4/10/ 2017