Decision Items for the Executive Committee About Google Workspace Settings

Item #	Decision Item	Affected Accounts	Staff Recommendation	Other Options	Discussion
1	Use of state resources	All "coleg.gov" accounts	By policy, members and staff should be advised not to respond to a campaign-related message from a coleg.gov account. They should respond in a separate email from a non-state provided account, with or without first forwarding the email. Staff recommends a footnote be placed on emails sent from member and district accounts that reads "State resources cannot be used for campaign purposes. Please do not send campaign-related content to this address."		
2	District accounts	District	Allocate one district account (e.g. Member.Aide@coleg.gov, i.e. Pugliese.Aide@coleg.gov) to each member. Allow credentials to a member's district account to be shared with aides actively employed by that member. Delegate a member's district account to the member's account, so that aides can help manage the member's email without giving aides access to member account credentials. By policy, designate members as the owners of their district account. Give member accounts delegated access to the district account email (i.e., the delegated access to email would go both ways).	Other options include: 1) Not providing district accounts (this option would save money relative to the current budget, although it is not recommended for security and accountability purposes); 2) Providing multiple generic district accounts (e.g. Member.Aide1@coleg.gov and Member.Aide2@coleg.gov) - this option would require a budgetary increase; and 3) Giving aides their own account (e.g. Firstname.Lastname@coleg.gov,) - this option would require a budgetary increase and would increase administrative workload.	Staff strongly recommends that aides receive district accounts for security and accountability purposes. Sharing member credentials with aides, especially when there is turnover, is a significant security risk. The collaborative functionality of Workspace should allow aides to fully perform the functions of their positions. Aides will be able to help manage member email through delegation, calendar through sharing calendar permissions, and drive files through a shared drive. Contacts, Tasks, Keep, and Sites can also separately be shared. However, aides will not be able to use Chat or Spaces as if they are the member. District accounts would provide an additional option for members to manage constituent email.
3	Password sharing	Member	By policy, prohibit members from sharing login information to their individual Workspace accounts with anyone, including an aide. Aides should be provided delegated access to the member account by logging into district accounts using district account credentials.	Allow members to share member account credentials with aides.	This is important for security and accountability. It will also create conditions that would protect the member's administrative authority for existing and future applications.

Decision Items for the Executive Committee About Google Workspace Settings

Item #	Decision Item	Affected Accounts	Staff Recommendation	Other Options	Discussion
4	CORA custodian	Member	Members remain custodians over their own data, including data in their Google Workspace accounts	1) Designate a nonpartisan agency director or specific nonpartisan position as the custodian (requires a bill)	Records include emails, Drive files, chat messages, Spaces messages, Group messages, Meet recordings and associated documentation, calendar events, etc.
5	CORA custodian	District	Designate members as the custodians over the data in their district account.	1) Designate the Secretary of the Senate or the Chief Clerk of the House as the custodian (requires a bill) 2) Designate a nonpartisan agency director or a specific nonpartisan position as the custodian (requires a bill)	Records include emails, Drive files, chat messages, Spaces messages, Group messages, Meet recordings and associated documentation, calendar events, etc.
6	Privacy	Member, District	By policy, prohibit LIS system administration staff from accessing data within member and district accounts, unless requested to do so by the member who owns the account.		Allowing LIS system administration staff access without permission is strongly discouraged.
7	Provisioning new legislators	Member, District	Assign both the member and district accounts to new legislators when they are provisioned with their state iPads and laptops at new legislator orientation.		There is room in the budget for the overlap between the election and the start of the next session.
8	Member account turnover	Member	Allow members to access their accounts for 60 calendar days following the day their successor is sworn in.	Allow members to access their accounts until their successor is sworn in, or after their successor is sworn in for a different amount of time than 60 days.	Should the Executive Committee choose to allow data to be migrated, 60 calendar days will allow time for members and LIS system administration staff to work together to ensure data migration is successful.

Decision Items for the Executive Committee About Google Workspace Settings

Item #	Decision Item	Affected Accounts	Staff Recommendation	Other Options	Discussion
9	Member account data migration	Member	Allow members to migrate their data into a personal account, subject to the technical limits of the receiving account. Allow migration to a successor member's coleg.gov account, upon request from the outgoing member.	Prohibit data migration	Member accounts will be deleted 60 days after the member's successor is sworn in (or after whatever period the Executive Committee chooses to grant outgoing members after they leave office). Once the account is deleted, Google allows LIS to recover the data for 20 days. Following the 20-day period, the data is deleted from the network and Google Vault. If there is a legal hold on the data because of a lawsuit or CORA request, that data can be archived in Google Vault. Google Vault is a data archive application that can be used to search for data within the entire coleg.gov instance and place holds on data in response to CORA requests or litigation holds. Access to Google Vault is tightly controlled and available only to specified LIS network system administrators.
10	District account - member turnover	District	Allow members to access their district accounts for 60 calendar days following the day their successor is sworn in.	Allow members to access their district accounts until their successor is sworn in, or after their successor is sworn in for a different amount of time than 60 days.	Should the Executive Committee choose to allow data to be migrated, 60 calendar days will allow time for members and LIS system administration staff to work together to ensure data migration is successful.

Decision Items for the Executive Committee About Google Workspace Settings

Item #	Decision Item	Affected Accounts	Staff Recommendation	Other Options	Discussion
11	District account - aide turnover	District	LIS will add or delete an aide's access to a district account only at the direction of the Secretary of the Senate or the Chief Clerk of the House, or their designee, as appropriate based on the employing member's chamber. Members must, by policy, be required to promptly communicate aide turnover to the Secretary or Chief Clerk. The Secretary or Chief Clerk, or their designee, should then create a helpdesk ticket with ithelp.ga@coleg.gov to request the addition or deletion. This must happen any time an aide enters into or leaves a specific member's employ, including when an aide leaves one member's employ to work for another member. Upon an aide's departure from that member's employ, LIS will reset the member's district account access to ensure continued access to the member and any other active aide. This will require a password change.		Ensuring that inactive employees no longer have access to district and, by delegation, member accounts is a significant security, confidentiality, and data loss prevention concern. Staff strongly recommends that leadership strictly enforce the requirement that members promptly communicate aide turnover to the Secretary of the Senate or Chief Clerk of the House, as appropriate.

Decision Items for the Executive Committee About Google Workspace Settings

Item #	Decision Item	Affected Accounts	Staff Recommendation	Other Options	Discussion
12	District account data migration	District	Allow data in a district account to be migrated to the member's personal account. Allow migration to a successor member's coleg.gov district account, upon request from the outgoing member. Prohibit district account migration to an aide's personal account.	Prohibit data migration	It is recommended that data in the aide accounts be, by policy, owned by the member. A member is an elected official, and not an employee. Migration should be prohibited to an aide's personal account because an aide is an employee. It is a generally accepted practice that employee data belong to the employer. Migration is unavailable for all employee accounts. District accounts will be deleted 60 days after the member's successor is sworn in (or after whatever period the Executive Committee chooses to grant outgoing members after they leave office). Once the account is deleted, Google allows LIS to recover the data for 20 days. Following the 20-day period, the data is deleted from the network and Google Vault. If there is a legal hold on the data because of a lawsuit or CORA request, that data can be archived in Google Vault.
13	Drive sharing	Member, District, Partisan staff	Allow documents to be shared with everyone, both internal and external		For security purposes, nonpartisan staff have stricter policies based on specifications from their senior leadership.
14	Chat sharing/access	Member, District, Partisan staff	Allow chat access to everyone, both internal and external		

Decision Items for the Executive Committee About Google Workspace Settings

Item #	Decision Item	Affected Accounts	Staff Recommendation	Other Options	Discussion
15	Chat history retention	Member, District, Partisan staff	Chat retention is set for the entire "coleg.gov" domain to 24 hours (chats are not saved until the next day). This setting can be customized for members and partisan staff.	Google Workspace allows this setting to be customized on an "operating unit" level within the Google instance. Member, district, and partisan staff are all contained within a single "operating unit" and therefore must all have the same setting. There are two settings available: 1) history off, which sets retention at 24 hours; or 2) history on, which allows chats to be retained indefinitely. If history is on for the operating unit, individual users can choose to turn history off for a particular chat within their account.	Nonpartisan staff cannot choose to retain chats for longer than 24 hours.
16	Spaces sharing/access	All "coleg.gov" accounts	Limit access/sharing in Spaces to internal "coleg.gov" accounts for all "coleg.gov" accounts. This setting cannot be customized for different user groups within the coleg.gov domain.	This setting cannot be customized for particular user groups, so any option would apply to the entire legislative branch, or all "coleg.gov" accounts. Two additional options available within Google settings include: 1) Turn sharing on, but only for whitelisted email domains (e.g. "state.co.us"). 2) Turn sharing on for all external email domains.	For security and confidentiality purposes, staff strongly recommend that the legislative branch prohibit sharing with external users in Spaces. The Legislative Management Team has discussed this setting for their staff and strongly prefers this setting. If whitelisting is allowed, staff strongly recommends not whitelisting domains such as "msn.com" or "gmail.com". Whitelisting these global domains is a significant security risk.
17	Spaces retention	All "coleg.gov" accounts	Spaces retention is set to 30 days for all "coleg.gov" accounts. This setting cannot be customized for different user groups within the coleg.gov domain.	This setting cannot be customized for particular user groups, so any option would apply to the entire legislative branch, or all "coleg.gov" accounts. Spaces retention setting can be set to either 24 hours (which is the setting for when history is turned off); or any amount of time 30 days or longer.	For security and confidentiality purposes, staff strongly recommend that the legislative branch prohibit retention beyond 30 days. The Legislative Management Team has discussed this setting for their staff and strongly prefers this setting.

Decision Items for the Executive Committee About Google Workspace Settings

Item #	Decision Item	Affected Accounts	Staff Recommendation	Other Options	Discussion
18	Calendar access: how much access do you want to give others to your primary calendar?	Member, District, Partisan staff	People can individually choose one of these three options: 1) Only share whether or not you are free or busy, and hide event details; 2) Share all information with users to whom you have granted those permissions, but these users cannot change your calendar. These permissions can be given to anyone with any Google account. 3) Share all information with users to whom you have granted those permissions, and allow these users to change your calendar. These permissions can be given to anyone with any Google account.	Make only one or any two of the three options available to member, district, and partisan staff accounts.	The Legislative Management Team has discussed this setting and decided that their staff should only be given the first option: to only share whether or not you are free or busy, and hide event details from other users. All three of the options shown in the recommendations column would be available to member, district, and partisan staff accounts, should the recommendation be adopted.
19	Automatic forwarding	Member	Automatic forwarding is allowed between any two "coleg.gov" accounts. Staff recommends that automatic forwarding from a member account to a specific external email address (any email address outside of the "coleg.gov" domain) be enabled upon request.	Prohibit automatic forwarding upon request from member accounts to email addresses outside of the "coleg.gov" domain.	Automatic forwarding is not managed within Google settings, but instead within the legislature's email security software "Proofpoint" settings. To enable automatic forwarding to an email address, LIS network administration staff must make a specific change within our Proofpoint instance. Automatic forwarding is a significant security, privacy, and data loss risk. The Legislative Management Team has discussed this setting and chosen not to allow it for nonpartisan staff.
20	Automatic forwarding	District, Partisan staff	Automatic forwarding is allowed between any two "coleg.gov" accounts. Staff recommends district and partisan staff accounts be prohibited from automatic forwarding to email addresses outside of the "coleg.gov" domain.	Allow automatic forwarding from district and partisan staff accounts to a specific email address outside of the "coleg.gov" domain upon request.	See the discussion for automatic forwarding from member accounts. Staff recommends treating staff differently because staff are employees, while members are elected officials and not employees. Most organizations strictly prohibit automatic forwarding from employee email accounts.