

## Data Management Policy

### 1.0 Purpose

To define access to various levels of the school's operating systems and provide for appropriate checks and balances to ensure confidentiality.

### 2.0 Google Vault Access

**Super Administrator:** Total access and authorization for all aspects of the Google Workspace, including all permissions described below and access to Google Vault. Authorized to initiate and close investigations, create holds, suspend accounts, and use all features. Password access and authorization for all aspects of the operating system, including Google Vault. Access via password utilized only in case of emergency when Network and Systems Administrator is unavailable.

Includes Network and Systems Administrator only.

Password is shared with (Executive Director(s) or Board President? - **tbd**)

**Vault Administrator:** Access to Google Vault. Authorized to initiate and close investigations, create holds, suspend accounts, and use all features. As needed, requested vault matters are shared by the Vault Administrator with appropriate individuals.

Network and Systems Administrator

**Custodian of Records (CORA request - ensure alignment with policy 1.16)**

Additional persons **tbd**

**Group Administrators:** Authorization for designated group. Includes permission to change group membership. Permissions defined by Administrator.

Registrars, Network and Systems Administrator

**User Management Administrator:** Authorization to add, remove, or suspend users  
(provide sample members with this designation)

**User:** A person granted access to vault records assigned to them for CORA requests or student-related issues. Access restricted to documents for which permission has been granted based on the circumstances.

Staff members or Board members as assigned by Executive Director(s) and/or Board President

**Services Administrator:** Permission to adjust features in Google Suite like turning on and off email or drive access. Authorization to create calendar resources like rooms and manage devices in the admin console.

**Tech Teachers/Front Desk:** Custom role allowing individuals to reset user passwords and move them between organization units.

The Administrator (assigned to Network and Systems Administrator only) maintains sole access to all drives and folders within the Google Workspace. The Administrator works with the Governance Board and Executive Director(s) to update access permissions when necessary. Requests from staff members or other members of the community, outside of normal procedures (i.e. elementary teacher requests access to elementary drive), must be directed through the President or Secretary of the Governance Board and/or the Executive Director(s).

## 2.1 Audits

The Network and Systems Administrator will run an audit log with two designated Board representatives each quarter. This audit log is available in the audit console of the Google Workspace. The logs will be stored in the Governance Drive.

The audit will also include a review of Distribution Lists for the Governance Board and underlying committees to ensure accurate representation.

## 2.2 Email Accounts

Due to FERPA and other privacy concerns, Google Workspace email addresses are provided only to Stargate employees (as defined in the Staff Handbook), Governance Board members, (and Governance Board committee chairpersons??). Authorization for other individuals is given only by permission of the Board President and/or Executive Director(s).

Discontinuation of Email Accounts:

Retired Governance Board members: The account is disabled and records are transferred to a suspended accounts folder.

Departed employees: The account is disabled, records are transferred to a suspended accounts folder, and any incoming emails are forwarded to the employee's manager. Any drive files associated with the account are shared with the employee's manager.

Graduating/departing students: Accounts are disabled following graduation or departure, then deleted the following year. The Google Vault automatically removes all data after the account is deleted.

2.3 Committee Emails - Committee email, the board liaison and committee chair will have access to the email, exceptions can be approved by the committee's board liaison. Upon the departure of a member or annually Board Liaisons will meet with the Information Technology Network Administrator to review email access.

## 2.4 Distribution Lists

The Network and Systems Administrator authorizes permissions for management of Distribution Lists. Permission to edit membership is usually granted to the committee chair or designated leader of the organization that the Distribution List represents. Upon the departure of a member or annually Board Liaisons will meet with the Information Technology Network Administrator to review email access.

## 3.0 Stargate School Records Management

Microsoft Sharepoint:

- Financial data accessible by the financial and accounting team only
- Payroll data accessible by financial, accounting, and Director of Human Resources
- Files from employee laptops and other school-owned computers are backed up to Sharepoint. Accessible by Network and Systems Administrator if needed, shared with other individuals as necessary for role transitions.

Local drive:

- Human Resources data accessible by the Director of Human Resources only

Google Suite:

- All other school records. Accessibility defined above

(Address backup of school files on employee laptops)