Stanmore Public School Parents and Citizens Association

Cloud Storage Access Control Policy

Cloud Storage Access Control Policy			
Effective Date	24 February 2015	**Policy Review**	2021
Responsibility	P&C Communications Committee	**Approver**	P&C Executive
Updated	28 February 2020	**Cross-Reference**	Code of Conduct

1. Policy Statement

Stanmore Public School Parents & Citizens Association [P&C] maintains Cloud Storage [Cloud] via a Google Drive [Drive]. This is to provide a centralised storage solution for all P&C related digital data allowing easy access to all current members of the P&C Executive, sub-committees and financial members with an active role on the P&C.

The intention is for current P&C members to use data stored within the Drive to assist them in their duties on behalf of the P&C. It is also expected that current P&C members will add to, update and enrich this data in any way that may benefit other members and future P&C members.

2. Background

Access controls are necessary to ensure only authorised current P&C members can obtain access to P&C data.

Access controls manage the admittance of users to the Drive by granting users access only to the specific resources they require to complete their role related duties.

Stanmore Public School shares data with the P&C on the understanding that that data is protected by access control methods and is only visible to authorised current P&C members who understand the sensitivity of the data that they have been granted access to.

3. Policy Objective

The P&C implements Role-based access control (RBAC) across the Drive in order to provide authorised and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability.

Access control systems are in place to protect the interests of all authorised users of the Drive by providing a safe, secure and accessible environment in which to share data with other P&C members.

Scope

This policy covers the P&C Cloud storage, Google Drive, data and authorised users.

4. Definitions

4.1. "Access Control" is the process that limits and controls access to resources of a computer system.

4.2. "System owner" is a member of the P&C Communications sub-committee with administrative responsibility for Cloud storage (including designating access) upon which P&C data resides.

4.3. "Cloud storage" is a model of computer data storage in which the digital data is stored on physical servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company.

4.4. "Google Drive" and/or "Drive" is a file storage and synchronization service developed by Google and accessible via the internet allowing users to store digital data on their servers, synchronize files across devices, create and share digital data.

4.5. "P&C members" are members of the P&C Executive, sub-committees and financial members with an active role on the P&C.

4.6. "Users" are P&C members who have requested and been granted access to the Google Drive and third parties that have been granted access to the Drive subject to provision 6.2.2.1. of this policy.

4.7. "Third parties" are individuals, groups or corporate entities that are not P&C members.

4.8. "Unauthorised users" are individuals, groups or corporate entities that may gain, have gained or been given access to the Drive and folders, files or data stored therein but which access has not been granted by the system owner.

5. Responsibilities

P&C Members

The P&C members that may have or require access to the Drive and P&C data contained therein are responsible for said data and the Cloud systems upon which the P&C data reside.

System Owner(s)

A member of the Communications sub-committee will be assigned the role of system owner.

If current members of the Communications sub-committee are unable or unwilling to become the system owner, the Executive will seek another P&C member to fulfil the role of system owner. If this is the case then such member will become a de facto member of the Communications sub-committee while they act as system owner.

6. Policy

6.1. Principles

Upon request, the system owner will provide any P&C members with access to the Drive and the data contained therein which they may need to carry out their P&C responsibilities in as effective and efficient manner.

6.1.1. Privileged accounts

The allocation of privilege rights (e.g. administrator, super-user) shall be restricted and controlled. The Cloud administration is the sole responsibility of the Communications sub-committee.

Authorisation for the use of such accounts shall only be provided explicitly, upon request from a member of the Executive, and will be documented by the system owner. The system owner shall not issue privilege rights lightly to guard against and prevent potential losses of confidentiality and/or integrity.

6.1.2. Least privilege and need to know

Access rights will be accorded following the principles of least privilege and need to know.

6.1.3. Maintaining data security levels

Every user should understand the sensitivity of their data and treat said data accordingly. Even if technical security mechanisms fail or are absent, every user should still attempt to maintain the security of data commensurate to said data's sensitivity.

Users electing to place information in the Drive should do so with the understanding that such information will be viewable by current and future P&C members. Users are consequently responsible in such situations for ensuring that data is appropriate for the audience and adheres to the P&C Code of Conduct.

Users should also take into consideration privacy when electing to place information into and share information from the Drive.

6.2. Access Control Authorisation

6.2.1. Access request

All current P&C members have the right to request access to the Drive.

The system owner reserves the right to decline access to the Drive without justification.

If access is declined the P&C member can raise an appeal with the P&C Executive. The P&C President has over-riding jurisdiction in such situations and their decision is final.

6.2.2. User accounts

Access to the Drive will be granted via the P&C member's personal Google account the details of which (e.g. Gmail address) will need to be provided to the system owner before access can be granted.

By default, user's access will be removed once their role on the P&C ends, unless a request for an extension is received by the system owner from the user or a current P&C member.

The system owner reserves the right to decline an extension of access to the Drive without justification.

If an extension is declined the user or P&C member can raise an appeal with the P&C Executive. The P&C President has over-riding jurisdiction in such situations and their decision is final.

6.2.2.1. *Third parties*

Third parties can be provided with accounts that solely provide access to the folder and/or data they are required to handle directly relating to P&C activities, in accordance with least privilege and need to know principles. Third party access must be requested by a current P&C member.

The system owner reserves the right to decline any such request without justification.

If said request is declined the P&C member that made the request can raise an appeal with the P&C Executive. The P&C President has over-riding jurisdiction in such situations and their decision is final.

Third party accounts will be removed when no longer required.

6.2.3. Passwords

It is the user's responsibility to protect their Google account password and other credentials to ensure the Cloud storage, Google Drive and data contained therein is not accessed by unauthorised users.

User's should not share their account password with anyone including the system owner.

6.2.4. Access to Confidential, Restricted and copyrighted information

'Confidential', 'Restricted' and copyrighted information should not be placed in the Drive unless required for the successful operation of the P&C and specific authority to do so is obtained from the information owner. Access to 'Confidential', 'Restricted' and copyrighted information should be limited to authorised users whose role responsibilities require it. The responsibility to implement access restrictions lies with the user who uploads the data and/or the system owner.

6.2.5. Policies and guidelines for use of accounts

Users are expected to become familiar with and abide by P&C policies, standards and guidelines for appropriate and acceptable usage of the Drive and data stored therein.

6.2.6. Sharing access to data on the Drive by users

Users agree not to share access to the Drive or any folders, files or data in any form, contained therein now or in the future, with any unauthorised users.

If P&C members believe third parties require access to the Drive or any folders, files or data therein they may request access be granted commensurate to section 6.2.2.1. of this policy.

The system owner reserves the right to decline any such request without justification.

If said request is declined the P&C member that made the request can raise an appeal with the P&C Executive. The P&C President has over-riding jurisdiction in such situations and their decision is final.

6.2.7. Access withdrawal

The system owner reserves the right to remove access to the Drive without prior notice. If access is withdrawn the user has the right to request access be reinstated through the usual channels.

If said request is declined the user can raise an appeal with the P&C Executive. The P&C President has over-riding jurisdiction in such situations and their decision is final.

6.3. Access Control Methods

Access to data is variously and appropriately controlled according to the folder / file classification.

Access control methods include providing explicit read / write access to the folders, files and data within the Drive relating to the user's role or activities on behalf of the P&C. Those users with read / write access to folders, files and data will be considered temporary 'custodians' of said data.

Role-based access control (RBAC) will be used as the method to secure access to all digital resources contained within the Drive.

Access to folders, files and data other than those relating to a user's role can be requested and may be granted, either temporarily or for the duration of the user's role, by the system owner. The system owner may seek specific authorisation from other P&C members who are considered owners of said folders, files and data before granting access.

The system owner reserves the right to decline any such request without justification.

If said request is declined the user that made the request can raise an appeal with the P&C Executive. The P&C President has over-riding jurisdiction in such situations and their decision is final.

6.4. Review and Development

This policy shall be reviewed and updated regularly by the Communications sub-committee as appropriate to ensure that it remains appropriate in the light of any relevant changes to the law, P&C policies or obligations. Any changes are subject to approval by the P&C Executive prior to implementation.

Additional regulations may be created to cover specific areas.