Procedure

OneSchool access management and use procedure

Version: 1.7 | **Version effective**: 20/12/2023

Audience

Department-wide

Purpose

This procedure outlines the responsibilities of departmental staff when using OneSchool and OneSchool Finance and the process for granting and managing the provision of user access to these systems.

Overview

OneSchool holds information that departmental staff in schools, regions and central office use to successfully and efficiently perform their duties.

As OneSchool contains sensitive and confidential information, it is essential that appropriate processes are in place to ensure:

- access to OneSchool is only granted to departmental staff who require access
- access is not granted to non-departmental employees, such as school-based youth health nurses, visitors, volunteers, school-based police officers, and chaplains
- approvers may not approve their own access
- access levels are necessary, appropriate and proportionate to a user's role
- ongoing monitoring to ensure OneSchool access is confined to those who require it
- the highest standards of confidentiality and privacy are maintained, with information disclosure only occurring where it is lawful and authorised.

Unauthorised OneSchool access or misuse of OneSchool information may result in disciplinary action under the Code of Conduct or department's Standard of Practice. This behaviour may also result in criminal prosecution under section 426 of the *Education (General Provisions) Act 2006* (Qld) and section 408E of the *Criminal Code Act 1899* (Qld).

Misuse or unauthorised access of OneSchool information, including those instances involving an undeclared and unmanaged conflict of interest, must be immediately reported to Integrity and Employee Relations (DoE

employees only). If misuse or unauthorised access involves a potential breach of privacy, this must be reported to the department's Principal Privacy Officer.

Responsibilities

Staff members requesting OneSchool access (requester)

- Only request access to OneSchool if access is necessary to perform their role.
- Request access that is appropriate and proportionate to the key tasks of their role, with reference to the OneSchool Access Level Guide (DoE employees only).

OneSchool users (user)

- Access and use information within OneSchool in compliance with the Code of Conduct, Standard of Practice, OneSchool User Access Agreement, legislation and the department's integrity and privacy policies and procedures.
- Maintain confidentiality and privacy of information accessed within OneSchool.
- Understand that OneSchool misuse or unauthorised access may result in disciplinary action and/or a criminal charge.
- Request access removal if access is no longer required, or is no longer appropriate and proportionate to the key tasks of their role.
- Request higher level or additional access if required, should key tasks change.
- Attention must also be given to the Internal Controls and Segregation of Duties (DoE employees only) guidance for finance roles.
- Report any suspected security incident or breach, inappropriate or disproportionate access, or misuse of OneSchool.

Endorsers (staff with line management responsibilities i.e. Head of Department, Deputy Principal, Assistant Regional Directors, etc)

- Verify that requested OneSchool access levels are appropriate and proportionate to the key tasks of a requester's or user's role, as outlined in the OneSchool Access Level Guide (DoE employees only), in centres where the Approver may not have clear and direct line of sight over all officers' roles.
- Make recommendations to the Approver about access requests.
- Support the Approver to review and monitor access.

Approvers (Assistant Directors-General, Regional Directors, Principal)

- Appoint a OneSchool System Administrator/s (SOSA/ROSA) to assist with management of user access and monitoring requirements.
- Nominate Endorsers for their centre if they do not have clear and direct line of sight over all officers' roles.
- Approve OneSchool user access and access levels where necessary, appropriate and proportionate.
- Ensure six-monthly reviews and ongoing monitoring of OneSchool user access and amend or remove access if required.

- Respond to and resolve any breach of the procedure, including removing user access and reporting potential breaches.
- Maintain records of approvals and review and monitoring activities.

Additional responsibilities for Regional Directors as Approvers

- Approve OneSchool user access and access levels for school principals where necessary, appropriate and proportionate.

OneSchool System Administrator (central office), School OneSchool System Administrators (SOSA) and Regional OneSchool System Administrators (ROSA)

- Provide advice about the functionality and access to information provided by specific OneSchool access levels.
- Support the Approver with actioning access requests and monitoring user access.

Process

Refer to the relevant OneSchool user access flowchart for information about different OneSchool user groups and how their access requests must be managed.

1. Request access

- The Requester considers the OneSchool Access Level Guide (DoE employees only) to determine:
  - if OneSchool access is **necessary** to perform their role
  - the level of access required that is **appropriate and proportionate** to the key tasks of their role.
- The Requester prepares and submits their OneSchool access requests using the functionality provided in OneSchool.
- A SOSA/ROSA/Central Office employee can set up the access request on behalf of an employee at their centre. The employee on whose behalf the access request has been created is notified via email and is then required to review their access request and progress on to the Endorser (or Approver).
- OneSchool access is requested in OneSchool, with the following exception:
  - Corporate and regional office users required to perform specific corporate tasks within the OneSchool finance module can request access (or changes to their existing access) by completing the Corporate OneSchool Finance User Access Agreement Form.
- As part of their request, the Requester must:
  - justify the level of access requested, based on the key tasks of their role
  - include an end date if access is only required temporarily
  - read and accept the conditions of access within the User Access Agreement.
- If an existing OneSchool user needs to amend their access levels, the above process will again be followed.
  - For example: access may need to be amended if a user is promoted, starts or ends temporary higher duties, or there are changes to their role or key tasks.

- All Requesters must direct their access requests to the designated Approver via an Endorser if required in their centre.

2. Consider access request, and decide to grant or refuse access

- When a request for access is received, the Endorser or Approver must make a decision about access based on an assessment of the following factors:
  - if access is **necessary** to enable the requester to undertake the key tasks of their role
  - if it is **appropriate** for the requester to have access to the types of information available within the access level requested
  - if the access level requested is **proportionate** by providing access to the minimal amount of information required to enable the requester to undertake the key tasks of their role.
- On consideration of these factors, the Endorser may decide:
  - requested access is not required: the Endorser will decline to endorse the requested access level/s
  - a lower level of access is required: the Endorser will decline to endorse requested access levels and advise the requester to re-submit a new request for a lower level of access
  - not all requested access is necessary, appropriate and proportionate: the Endorser will endorse specific access level/s and decline to approve others.
  - requested access is necessary, appropriate and proportionate: the Endorser will endorse requested access level/s.
- If the Endorser decides that access is necessary, appropriate and proportionate, their recommendation about access is progressed to the Approver, who must also consider the factors above and decide whether to approve provision of the requested access level/s.
- In a school, the SOSA can approve school access level requests on behalf of a principal.
- Access is granted through OneSchool once the request is approved.
- The staff member who has requested access will be notified by email whether access has been approved.
- All access requests are automatically recorded in OneSchool.

3. Use of OneSchool

- All OneSchool users must use the system in accordance with the User Access Agreement (this is an electronic agreement displayed when accessing OneSchool for the first time), Code of Conduct and department's Standard of Practice, and departmental policies and procedures. OneSchool users must:
  - only access information that is directly relevant to undertaking the key tasks of their role
  - not disclose personal information obtained through OneSchool without first ensuring they have lawful authority to do so
  - maintain the confidentiality and privacy of information obtained in OneSchool, including when they are no longer employed by the school/department
  - maintain OneSchool security by taking precautions to prevent unauthorised access, such as locking devices and logging out of OneSchool

- not enter false information or falsify student records
- notify their Endorser or Approver immediately if they detect a possible security incident or breach, inappropriate or disproportionate access to OneSchool, or misuse of OneSchool information
- notify their Endorser or Approver immediately if they detect misuse or unauthorised access of OneSchool information, including instances involving undeclared and unmanaged conflict of interest.

- If misuse of OneSchool or unauthorised access to OneSchool information is reported or identified, the Approver must immediately:
  - remove, or arrange removal of, the user's OneSchool access and advise the user why this has occurred
  - report the suspected breach to Integrity and Employee Relations and/or the department's Principal Privacy Officer (if the breach concerns privacy).

4. Review and monitoring of access

Review

- The Approver must review OneSchool user access every 6 months.
  - Reviews are to be conducted using the access review functionality in OneSchool. The Approver may conduct the review personally, or they may arrange for delegates to conduct the review and provide recommendations to the Approver to inform their decisions about whether users should retain their current access levels.
- Reviews must consider each user within the Approver's area of responsibility to decide:
  - if access remains **necessary** to enable the user to undertake the key tasks of their role
  - if it remains **appropriate** for the user to have access to the types of information available within their current access level
  - if the access level remains **proportionate** in terms of providing access to the minimal amount of information required to enable the user to undertake the key tasks of their role.
- The Approver or System Administrator may need to request information from the user to inform the decision.
- If the Approver decides a user's access needs to be amended or removed, they must, as soon as reasonably practicable:
  - amend or remove the user's access in OneSchool, or arrange for this to be undertaken by the System Administrator.

Ongoing monitoring

- The Approver must have local processes in place to ensure any OneSchool user access that is inappropriate, disproportionate or no longer necessary can be detected and promptly addressed outside of the six-monthly review cycle. This includes the following situations:
  - **Removing access if a user leaves the department**: the Approver must remove or arrange for removal by the User or System Administrator, of a user's access as part of the employee separation process. A User may also remove their own access if required.

- **Changing or removing access if a user's role or key tasks change**: the user must request amendment or removal of access levels as soon as possible after their role or key tasks change, in accordance with Process step 1 above. As a contingency, the Approver must also regularly monitor access levels to detect and address any changes to a user's role or key tasks that have not been reported by a user.
- **Removing access if inappropriate use or access is detected**: the Approver must immediately remove, or arrange for removal, of the user's access and report the suspected breach, in accordance with Process step 3 above.

Definitions

Term	Definition
Access request	The method used to request OneSchool user access which provides reasoning for access. Access is approved by the principal of the school, Regional Director of the Region or Assistant Director-General and is kept as a record.
Additional access	User access privileges that enable a user to undertake specific tasks within OneSchool (e.g. playground duty administration, school calendar management, timetable administration, etc.).
Approver	The Officer-in-Charge in a centre who is accountable for the approval of OneSchool user access provision and review (i.e. principal, Regional Director, Assistant Director-General).
Endorser	A OneSchool access level intended for use in larger centres in which the Approver may not have clear and direct line of sight over the key tasks of all officers' roles in that centre. The centre's Approver may allocate the access level to officers who have line management responsibilities in that centre and who are therefore able to confirm the appropriateness and proportionality of access levels to the key tasks of a user's role.
Key tasks	A specific component of the work conducted within a user's job duties as outlined in their role description.
OneSchool	OneSchool is a comprehensive software program that enables Queensland state schools to efficiently and effectively manage key teaching and school administrative activities, as well as the ongoing support of students.
OneSchool Access Level Guide	The OneSchool Access Level Guide defines school, corporate and regional based access level privileges. The information in the guide presents an aggregation of user access privileges necessary and sufficient for the performance of the functions of a specific job (e.g. classroom teacher, Head of Curriculum, Business Manager, principal etc).

Term	Definition
OneSchool Finance application	The OneSchool Finance application is a third-party application integrated with OneSchool to support financial management functions, such as invoicing and asset management.
OneSchool access level	An aggregation of user access privileges necessary and sufficient for the performance of the functions of a specific job (e.g. classroom teacher, Head Of Curriculum, Business Manager, principal, etc.).
Regional OneSchool System Administrator	The Regional Director's nominee who is responsible for supporting OneSchool user access privileges and compliance.
School OneSchool System Administrator	The principal or principal's nominee who is responsible for supporting OneSchool user access privileges and compliance.
OneSchool System Administrator (Central Office)	The OneSchool support team is the nominee for supporting OneSchool user access privileges and compliance.

Legislation

- *Education (General Provisions) Act 2006* (Qld) section 426
- *Information Privacy Act 2009* (Qld)
- *Criminal Code Act 1899* (Qld) s 408E
- *Crime and Corruption Act 2001* (Qld)
- *Human Rights Act 2019* (Qld)
- *Public Sector Ethics Act 1994* (Qld)
- *Public Sector Act 2022* (Qld)
- *Public Interest Disclosure Act 2010* (Qld)
- *Integrity Act 2009* (Qld)

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Nil

Supporting information for this procedure

- OneSchool user access flowchart

Other resources

- Information security policy
- Information privacy and right to information procedure
- Information security procedure
- Code of Conduct for the Queensland public service
- Standard of Practice
- Conflict of interest procedure
- Reporting fraud and corruption procedure
- Making and managing a public interest disclosure procedure
- Fraud and Corruption Control Framework (DoE employees only)
- Personal information guideline
- Identity and access management guideline
- OneSchool access level guide (DoE employees only)
- Internal Controls and Segregation of Duties (DoE employees only)
- Information Security Classification Framework
- Queensland Government Enterprise Architecture Information security policy
- Crime and Corruption Commission

Contact

For further information, please contact your closest regional office.

Review date

5/10/2024

Superseded versions

Previous seven years shown. Minor version updates not included.

1.0 OneSchool access management and use procedure

Creative Commons licence