Government of **Western Australia**
School Curriculum and Standards Authority

Research Governance Policy and Policy Principles for Research Governance

DOCUMENT INFORMATION	
Responsible Officer	Manager, Strategic and External Relations
Document type	Policy
Status	Published
Last review date	13/10/2022
Next review date	13/10/2024
HPRM number	2019/3962[v7]

Acknowledgement of Country

Kaya. The School Curriculum and Standards Authority (the Authority) acknowledges that our offices are on Whadjuk Noongar boodjar and that we deliver our services on the country of many traditional custodians and language groups throughout Western Australia. The Authority acknowledges the traditional custodians throughout Western Australia and their continuing connection to land, waters and community. We offer our respect to Elders past and present.

School Curriculum and Standards Authority
303 Sevenoaks St CANNINGTON WA 6107
PO Box 816 CANNINGTON WA 6987

Telephone: +61 8 9273 6300
Facsimile: +61 8 9264 6371
Email: info@scsa.wa.edu.au
Web: www.scsa.wa.edu.au

2019/3962[v7]

This document contains the following:

Document 1:
Research Governance Policy (Policy)

Document 2:
Policy Principles for Research Governance (Policy Principles)

Policy maintenance
This Policy and corresponding Policy Principles are to be reviewed and updated every two years (or where necessary). Any revisions to this Policy and/or Policy Principles must be submitted for consideration and approval by the Responsible Officer to executive management of the School Curriculum and Standards Division, and the School Curriculum and Standards Authority (the Authority) Board.

Date	Alteration	Rationale	Officer/s editing
13/10/2021	Inclusion of references to risk of cultural harm, de-identified information application review and Board member feedback.	Changes made to respond to stakeholder feedback and reflect current state.	Ben Businovski

Contents

1. Policy statement

The School Curriculum and Standards Authority (the Authority) aims to support research that is connected with promoting student achievement and wellbeing, or understanding outcomes connected with student achievement or wellbeing. In support of this aim, the Authority facilitates the disclosure of information for the purposes of research involving students.

The *Research Governance Policy* (Policy) and supporting *Policy Principles for Research Governance* (Policy Principles) set out the Authority's approach and requirements pertaining to requests for the use, retention and disposal of Authority information for the purpose of research involving students to ensure that:

- an applicant requesting information has demonstrated the benefits of their research project in terms of its contribution to student educational outcomes and/or wellbeing
- there is a need for identified student information for the purpose of research
- the Authority acts in accordance with relevant legislative and regulatory requirements
- an applicant who receives student information will be held accountable for the use, retention and disposal of this information.

This Policy also sets out:

- lodgement procedures applicable to research requests for Authority information
- principles applicable to the receipt, retention and handling of student information obtained from the Authority.

2. Scope

This Policy applies to the Authority Board, individuals or staff acting for and on behalf of the Authority, and applicants.

3. Background

An applicant wishing to access student information as part of a research project can submit an application to the Authority for access to such data held by the Authority. The fields of information applicants can access are detailed in Section 2.2 of the Policy Principles. This Policy sets out the Authority's approach to decision making with respect to applications for student information (defined below) and managing the disclosure and use of information by applicants to ensure that:

- access to the Authority's information is granted to approved applicants in accordance with legislative requirements
- applicants who receive information abide by the Authority's access conditions and principles.

In addition to reviewing applications for student information, the Authority has the responsibility of monitoring approved applications to ensure that:

- applicants adhere to the conditions stipulated in their *Agreement for the disclosure of information*
- the information disclosed to applicants is used in accordance with the requirements stated in this Policy and the accompanying Policy Principles document.

4. Key terms

Applicant	An individual who has lodged an application requesting information from the Authority for the purposes of research. This individual will typically be applying on behalf of the Principal Researcher. An applicant can also be the Principal Researcher.
Application	A request made to the Authority for the disclosure of relevant information under section 32B of the *School Curriculum and Standards Authority Act 1997* to conduct research involving students.
Ethics Review Committee (ERC)	The Ethics Review Committee is appointed by the Authority Board and is responsible for reviewing each application for information disclosure, and making a recommendation to the Authority Board, in consideration of the factors described in this Policy on whether to approve the disclosure of information for research purposes.
Harm	That which adversely affects the interests or welfare of an individual or a group. Harm includes, but is not limited to, physical harm, cultural harm or damage, anxiety, pain, psychological disturbance, devaluation of personal worth and social disadvantage.
Information Breach	See section 4.1.
Principal Researcher	A person who is responsible for managing the use of relevant and/or personal information obtained from the Authority through the information disclosure process. A Principal Researcher must be enrolled in or hold a Masters Degree or higher.
Research	An investigation, centred on a research question or questions, undertaken to gain knowledge and understanding in relation to either or both of the following purposes: • promoting student achievement or student wellbeing • understanding outcomes connected with student achievement or wellbeing.
Research Officer	An individual appointed to support the Authority's information disclosure for research function.
School Curriculum and Standards Authority (the Authority)	The School Curriculum and Standards Authority is a body corporate constituted under the *School Curriculum and Standards Authority Act 1997* (WA).
Student	A student enrolled in a school or receiving home education.
Student Information	Information about an individual who is a student, listed in Section 2.2 of the Policy Principles.
Wellbeing	Wellbeing of a student includes the following: • care of a student • cultural and community wellbeing of a student • the physical, emotional, psychological or educational development of a student • the physical, emotional or psychological health of a student • the safety of a student.
Working with Children Check (WWC)	The Working with Children (WWC) Check is a compulsory screening strategy in Western Australia and the Christmas and Cocos (Keeling) Islands for people who engage in certain paid or unpaid work with children, described as 'child-related work' under the *Working with Children (Criminal Record Checking) Act 2004* (the WWC Act).

5. Relevant documents and other sources of information/websites

5.1 State-based legislative and other regulatory frameworks

School Curriculum and Standards Authority Act 1997
School Curriculum and Standards Authority Amendment Act 2017
School Curriculum and Standards Authority Regulations 2005
School Curriculum and Standards Authority Amendment Regulations 2020
Health Services (Information) Regulations 2017

5.2 National legislative and regulatory frameworks

National Statement on Ethical Conduct in Human Research (2007) (updated 2018)
Australian Code for the Responsible Conduct of Research (updated 2018)
Values and Ethics – Guidelines for Ethical Conduct in Aboriginal and Torres Strait Islander Health Research
Privacy Act 1988 (Cth)

5.3 Policy and Procedural Frameworks

Department of Education. (2020). *Working with Children Checks in Department of Education Sites Policy and Procedures.* Department of Education, Perth.
Department of Health. (2021). *WA Health Research Governance Policy and Procedures,* Research Development Unit, Department of Health, Perth.
Department of Health. (2017). *Department of Health Western Australia Human Research Ethics Committee Standard Operating Procedures,* Department of Health, Perth.
Department of Health. (n.d.). *Application process*, Data Linkage WA, Perth.
Department of Health. (2014). *Practice Code for the use of personal health information* provided by the Department of Health, Department of Health, Perth.
Department of Health. (2010). *Managing Conflicts of Interest Policy*, Department of Health, Perth.
Office of the Australian Information Commissioner. (2018). *Notifiable Data Breaches scheme*, Office of the Australian Information Commissioner, Sydney.

5.4 Research Governance Forms

Application for disclosure of information form (2021/13961[v2])
Application for disclosure of information amendment form (2018/29564[v2])
Conflict of interest form (2021/42103)
Declaration of confidentiality form (2018/29563[v3])
Agreement for the disclosure of information (2021/49648[v4])
Annual report form (2018/29567[v2])
Information breach notification form (2018/29569[v2])
Information disposal acknowledgement form (2018/29571[v2])
Ethics Review Committee Terms of Reference (2021/63670[v2])

Research Governance Policy and Policy Principles for Research Governance

1. Policy Principles

These Policy Principles are to be read in conjunction with the *Research Governance Policy*. These Policy Principles are mandatory and set out the following:

- process for the submission, review and approval of applications for disclosure of information
- principles covering the use, retention and disposal of information.

2. Process for the submission, review and approval of applications for disclosure of information

Queries from applicants regarding the following stages of the process can be directed to the Research Officer at research@scsa.wa.edu.au.

2.1 Applicants

Applicants wishing to submit an application for student information from the School Curriculum and Standards Authority (the Authority) for the purposes of research are to comply with the requirements detailed in this Policy Principles document.

Applicants must have experience, skills and qualifications commensurate with the proposed research project for which information disclosed by the Authority is required. The expertise of researchers will be taken into consideration by the Authority Board in making a decision on an application for information. Applicants must also have a valid Working with Children (WWC) Check throughout the duration of the research.

2.2 Fields of information

For the purposes of research, applicants can lodge an application for the following fields of information:

- student name
- address
- date of birth
- gender
- student number
- Aboriginal or Torres Strait Islander status
- main language spoken by a student at home
- main language spoken by a student's parents at home
- educational programs or courses in or for which a student was most recently enrolled or receiving home education
- educational programs or courses in or for which the student was previously enrolled or receiving home education
- the student's educational achievement
- whether the student is or was participating in an option other than school in accordance with the *School Education Act 1999* (WA) section 11B.

The Authority will not disclose information other than the fields listed above. Requests for de-identified information will contain anonymised versions of the above fields.

2.3 Application periods

The Authority processes applications for access to student information for the purposes of research quarterly in a calendar year.

Specific opening and closing dates for each application round will be published on the Authority's website (www.scsa.wa.edu.au) in advance of these periods.

The Authority reserves the right to prioritise applications at their discretion, where no actual or perceived conflict of interest exists.

2.4 Lodgement of application

An applicant who wishes to lodge an application for the disclosure of student information must submit a completed application through the Authority's website.

It is an applicant's responsibility to ensure that their application is complete, and all supporting documents are attached. Incomplete or late applications will not be accepted.

An applicant may withdraw their application at any stage of the application process by informing the Research Officer in writing at research@scsa.wa.edu.au.

Applications that have been withdrawn and subsequently resubmitted will be regarded as new applications.

2.5 Estimate of costs

Applications made to the Authority for the disclosure of student information under this Policy will be subject to a fee. A standard fee will apply to requests for prepared information, and the cost will vary according to the complexity of customised information requests.

Estimates are provided to assist applicants with research budgeting and may not reflect the final cost of receiving information from the Authority.

Charges levied by the Authority for the disclosure of student information are contingent on the scope, format and complexity of an application. Potential applicants are encouraged to contact the Authority prior to submitting an application to discuss costs.

Additional fees for approved changes to the scope of an application may apply.

2.6 Application review process

An applicant will receive written confirmation after their application has been submitted to the Authority. Applications for identified information will be vetted by Authority staff for completeness and reviewed by an Authority Board-appointed Ethics Review Committee (ERC) who will consider, at a minimum, whether the applicant can implement and adhere to the principles and practices of appropriate ethical standards in human research.

The ERC is appointed by the Authority's Board under the directions of the *School Curriculum and Standards Authority Amendment Regulations 2020* (the Regulations). The ERC shall be comprised of at least five individuals who have the necessary skills and expertise to evaluate an applicant's request for student information and may include:

- a suitable person determined by the Authority's Board (who shall be Chair of the ERC)
- an executive management officer of the Authority
- a lawyer with expertise in privacy or information sharing
- a professional with expertise in psychology or children's development and wellbeing
- a community figure also acting as a layperson
- a person having suitable status and of Aboriginal background
- a researcher with expertise in research ethical applications and compliance
- an executive management officer of the Department of Communities
- an executive officer from the Authority (non-voting).

The ERC operates within the settings and requirements of the *ERC Terms of Reference*. The ERC will assess applications received by the Authority in accordance with the following points:

- whether the application for the information meets the criteria of Section 32B(3) of the *School Curriculum and Standards Authority Act 1997* (the Act)
- whether potential risks to individuals' safety can be justified in the context of the benefits of an applicant's research. These benefits may include
  - an original contribution to knowledge that promotes student achievement or wellbeing
  - an original contribution to knowledge that benefits an understanding of outcomes related to student achievement, wellbeing or both
- whether the applicant has received approval from a Human Research Ethics Committee (HREC) registered with the National Health Medical Research Council (NHMRC), including
  - where applicants do not have HREC approval, the ERC will only consider applications that carry no more than low risk as defined under paragraphs 2.1.6 and 2.1.7 of the *National Statement on Ethical Conduct in Human Research* (the National Statement)
  - low-risk applications will be reviewed in relation to the criteria set out in paragraphs 5.1.18 to 5.1.23 of the National Statement, which broadly cover research integrity, risk, benefit, privacy, consent and ethical considerations
  - applications without HREC approval that do not address the preceding two points to the satisfaction of the ERC will not be recommended for approval until applicants either obtain HREC approval or address the preceding two points
  - where applicants do have HREC approval, the ERC will assess whether the application abides by the national legislative instruments and guidelines that pertain to ethics and privacy, such as the National Statement and *Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: Guidelines for researchers and stakeholders.*
- whether the disclosure of student information is reasonably necessary for the applicant's research project
- whether, for the student information requested in a given application, it is impracticable to obtain consent from the individuals to whom the student information relates to
- whether an applicant can comply with the conditions stipulated in the Authority's information disclosure contract, and any written law, guideline or policy that applies to their research.

By addressing the above criteria, the ERC is to provide a recommendation to the Authority Board to determine whether an application should be approved, rejected or approved conditionally.

Applications from Western Australian State Government bodies may be reviewed directly by the Board on a case-by-case basis. Applications for de-identified information will be reviewed by an internal panel of Authority staff members and may be referred to the ERC. Applicants will be informed of the outcome of their application(s) and receive feedback from the Authority.

2.7 Refusals

The Authority reserves the right to refuse applications lodged for reasons it deems appropriate. The reasons may be an applicant's inability to sufficiently address one or more of the criteria set out in section 2.6 of these Policy Principles. Written advice addressing the reason(s) for a refusal will be provided to an applicant.

2.8 Protection orders

Where the Authority has been notified that a protection order is made for a student by the Department of Communities – Child Protection and Family Support, a Magistrate or other entity having legal authority to do so, the Authority will not disclose information about the student for the purposes of research inconsistent with the protection order. Where doubt arises regarding the application of a protection order, the Authority will seek advice from relevant agencies and/or the State Solicitor's Office (SSO).

2.9 Variation requests and deferred decisions

The Authority Board may offer conditional approval of an application under the following circumstances:

- it imposes a condition that a variation be made to the parameters of an application
- approval is given to an application once further information is submitted to the satisfaction of the ERC Chair and the Authority's executive management group.

Student information shall not be disclosed until the requirements of conditional approval are met to the satisfaction of the Authority's Board.

2.10 Conflicts of interest

The Authority requires applicants to disclose all actual, perceived or potential conflicts of interest in the *Declaration of confidentiality form*.

Conflict of interest situations may arise where an individual is put in a position where their ability to act independently and/or ethically without prejudice may be, or appears to be, compromised by self-interest or a relationship with a third party.

Applicants must describe how they will manage these conflicts of interest. Applicants who fail to declare conflicts of interest may be considered to be in breach of their *Agreement for the disclosure of information,* and penalties may apply.

2.11 Post-approval procedures

Applicants are required to comply with all Authority requirements for the release of information, which are detailed in the following sub-paragraphs.

2.11.1 Schedule of charges

Approved applicants will be provided with a schedule of relevant information disclosure costs that pertain to their application. Applicants must pay their charges for information disclosure and have their *Declaration of confidentiality form* and *Agreement for the disclosure of information* approved by the Authority prior to information being disclosed. These charges are non-refundable after services are rendered. The fees levied by the Authority for the disclosure of student information

follow a cost-recovery principle. Charges are based on the operational costs to the Authority for reviewing and processing requests. The Authority will review such costs at least annually.

2.11.2 Agreement for the disclosure of information

Approved applicants are required to enter into a contractual arrangement by signing the *Agreement for the disclosure of information* with the Authority that stipulates conditions for the use, retention and disposal of information. An applicant must sign and return to the Authority the *Agreement for the disclosure of information* prior to student information being disclosed. Applicants will also be required to sign the *Declaration of confidentiality form*. Applicants must comply with the Authority's requirements relating to the use, retention and disposal of information detailed in Section 3 of these Policy Principles.

2.11.3 Amendments to approved applications

An applicant is required to keep the Authority informed of any significant changes to a project. These charges may relate to the conduct of research or ethical aspects of a project, including:

- changes to the maintenance and security of information
- changes to an applicant's ability to comply with the Authority's conditions
- changes to a project's scope (for example, personnel changes, changes in research direction, alterations to information used)
- termination or suspension of a project
- information breaches or adverse events.

Applicants may make amendments to their application for information obtained from the Authority through the *Information disclosure application amendment form*. Applications for amendments will be considered by the Authority Board on a case-by-case basis. Depending on the scope of amendments required, an applicant may be required to provide the Authority with additional supporting material and pay additional costs.

Applicants are also required to inform the Authority if research projects are discontinued or completed before the expected date of completion.

2.11.4 Publications relating to research

As part of their application, applicants must inform the Authority of how their research will be published and maintain the confidentiality of individuals, schools and education sector/systems.

2.11.5 Disposal of information

When an applicant has concluded their research project, or the retention period has lapsed, applicants are required to dispose of the information obtained from the Authority. This must be completed in accordance with the disposal plan outlined in the submitted *Information request application form*. The applicant must also submit a completed *Information disposal acknowledgement form* and a final *Annual report form* to the Authority after their research project has concluded.

2.11.6 Complaints

Complaints involving approved applicants' use of student information may be lodged with the Authority. Individuals seeking to lodge complaints about any aspect of an approved applicant's

conduct may contact the Research Officer directly. The Authority will address complaints in accordance with its complaints management procedures.

2.11.7 Authority's Annual Report and register

The Authority will publish information about the number, nature and outcome of applications accepted by the Authority Board in its Annual Report. The nature of applications will include the broad categories of demographic, enrolment and achievement information.

The Authority will also maintain a register of applications that contains information pertaining to each application lodged with the Authority, whether formally accepted or not. The register will be managed in accordance with the Authority's records management procedures. The register will contain the following details for each request:

- the name of the applicant
- the date on which the request was submitted
- if the request was accepted under regulation 31 – whether the request was approved or refused by the Board
- if the request was approved – the type or types of relevant information disclosed by the Board.

2.11.8 Information breaches and adverse events

The Authority must be informed if there is a breach resulting in the disclosure of information to unauthorised individuals. Breaches must be reported within 48 hours by submitting a completed *Information breach notification form* to the Authority's Research Officer at research@scsa.wa.edu.au.

To ensure that breaches are dealt with in an appropriate manner, applicants must treat breaches in accordance with the Information Breach Protocol in Section 4 of these Policy Principles.

3. Principles for use, retention and disposal of information

The following principles related to the use, retention and disposal of the Authority's information need to be adhered to by an approved applicant.

3.1 Principles for use of information

To ensure that the information disclosed to applicants is only used for the authorised research purpose, the following principles apply:

- All individuals having access to particular information must be specified within the application.
- Access must only be given to those who are using the information for purposes outlined in the application.
- Authorised users must not disclose student information without prior written approval from the Authority.
- Any changes in individuals involved in the research project that use or will use student information must be documented and approved by the Authority.
- Authorised users must ensure the protection of information received from the Authority against theft, loss, unauthorised access, use, disclosure and unauthorised copying or modification.

- Information obtained from the Authority must not be used to identify or contact any individual or merged with any other information held by the user without prior approval from the Authority.
- The information obtained from the Authority must only be kept for the period approved by the Authority.
- Information required for a longer time period than specified in the relevant application must be approved in writing by the Authority.
- At the end of the retention period specified in an application, the information held by the applicant must be disposed of securely and in accordance with the disposal requirements of the Authority outlined in Section 2.11.5.
- As part of their application, applicants must enter their Information management and security plan.

3.2 Principles for retention of information

Applicants are required to comply with the following requirements pertaining to the storage, transportation and retention of information received from the Authority:

- When portable computer and storage devices are used for the transport of information, the information must be transferred to primary storage (e.g. a workstation or computer that is used to analyse information) as soon as practicable.
- The Authority's information may only be stored on cloud-based data storage, where such storage is on Australia-situated servers.
- The Authority's information may only be kept for the approved period specified in the information access duration section of the application form.

The Authority will review security plans as part of the application approval process. An applicant's security plans should address the following (further discussed in following subsections of these Policy Principles):

- physical/environmental security
- technological security
- transportation security
- privacy.

3.2.1 Physical/Environmental security

Applicants must ensure the physical and environmental security of hardware and storage media. Physical and environmental access controls should be managed by applicants to restrict access to data and may include:

- restricting access to locations where data is stored using physical security passes
- locking servers in rooms with access restrictions
- positioning work areas to prevent unauthorised access or viewing of information
- keeping storage devices in a secure location
- maintaining registers of access to devices storing student information.

Hardcopy records of student information received from the Authority should only be created when necessary, stored securely and disposed of in accordance with the disposal plan outlined in the

submitted *Information request application form*. Access must only be given to those who are using the information for the purposes outlined in the original application.

3.2.2 Technological security

Applicants must ensure that appropriate technological security measures are in place. For example:

- Applicants should have appropriate password management protocols.
- Computers are secured with firewalls and automatic screen locking mechanisms.
- Access to computers that contain information is restricted solely to researchers working on the research project.
- Encryption protocols are followed for student information when information is stored, archived or transferred across devices.
- Networks on which student information is stored are secured and remote access restricted.
- Electronic devices have appropriate virus and malicious software protection.
- Servers and databases are patched regularly.
- Access is only given to those who are using the information for the purposes outlined in the approved application.

3.2.3 Transportation security

Student information that is transported from one location to another must adhere to the following requirements:

- Student information transported from one location to another must be kept to a minimum.
- Student information must be password protected.
- Student information must be encrypted.
- Encryption keys must be stored on separate devices when being transported.
- Authorised personnel must not leave storage devices unattended.
- Student information must only be transported by authorised personnel.
- Student information must not be transmitted across unsecured networks.

Electronic transmission of student information must abide by the following requirements:

- The Authority needs to approve the transmission and security methods stipulated in the applicant's Information management and security plan.
- Student information must only be transferred between approved secure locations.
- The volume of student information transferred must be kept to a minimum.
- Transmission must be made via secure file transfer processes.

3.2.4 Privacy

Applicants must ensure the privacy of information disclosed by the Authority is managed in respect to Parts 1 and 3 of the *Office of the Australian Information Commissioner Australian Privacy and Principles Guidelines* or Schedule 1 of the *Privacy Act 1988 (Cth).*

3.3 Principles for disposal of information

During the application process, an applicant must enter details of a disposal plan to the Authority, outlining how information provided by the Authority will be returned or destroyed by the applicant.

The approved disposal plan will be referenced in the applicant's *Agreement for the disclosure of information*. The disposal plan must, at a minimum, include the following details:

- when the student-related information is to be destroyed
- how the information is to be destroyed
- who will authorise the destruction of the information
- who will be responsible for destroying the information
- how destruction of the information will be confirmed
- how confirmation of information provided by the Authority that appears in secondary information will be disposed of.

Destruction of student information provided by the Authority means that any such information either in its original form or any derived form in paper, electronic, or any other medium, including back-up copies, must no longer exist following the destruction activity.

Student information must be removed from all electronic storage devices and all files deleted in such a way that the contents of files are destroyed.

Paper records must be shredded or pulped for secure waste disposal. Disposal should be carried out as indicated in the applicant's disposal plan.

Applicants are expected to adhere to their disposal plans. Non-compliance with these plans may be construed as a breach of an applicant's *Declaration of confidentiality form* and *Agreement for the disclosure of information*. The Authority may conduct an audit or inspection of an applicant's disposal arrangements periodically.

4. Information breach protocol

4.1 Breach definition

An information breach happens when personal information is accessed or disclosed without authorisation or is lost. Information breaches occur when student information is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether unintentionally or intentionally. Breaches can be caused by a variety of factors and give rise to a range of varying consequences. Breaches include incidents where there is a material risk that a breach may occur.

A list of possible information breaches are as follows:

- improper handling of information obtained from the Authority
- an agency or organisation inadvertently providing student information to the wrong person
- an individual obtaining information through misleading and deceptive conduct
- lost or stolen media devices, such as laptops and storage devices or hardcopy records containing student information
- unauthorised publishing to an uncontrolled environment
- unauthorised access to records or electronic databases
- unauthorised disclosure of student information that has the potential to cause an adverse event
- an environmental or physical breach occurs, where information management facilities are not located in an environment that provides appropriate and/or secure operating conditions

- other unforeseen events that may affect the ethical acceptability of the use of student information provided by the Authority.

An applicant must take the necessary steps to contain, minimise the effect of, or stop an information breach when it occurs. The applicant must also collect information about the breach and submit an *Information breach notification form* to the Authority's Research Officer at research@scsa.wa.edu.au **within** 48 hours of the breach occurring. Each breach will need to be dealt with on a case-by-case basis in accordance with the protocols outlined below.

4.2 Responding to breaches

The person who discovers the breach must immediately initiate a containment process by taking steps to contain the breach. Applicant processes for responding to breaches must include the following steps where applicable:

- determining what information has been disclosed
- taking steps to contain the breach and minimise the impact of the breach
- retrieving as much of the information that has been disclosed
- collecting as much information about the cause, effect and actions taken with regards to the breach
- preventing further unauthorised access to student information or stopping an unauthorised practice
- if there is a risk of harm to an individual or individuals, those affected should be notified immediately
- determining the ramifications of the breach and taking steps to prevent further harm to individuals or further disclosure of information
- establishing a prevention plan to prevent future breaches.

At the same time, an individual who is made aware of a breach should assess the nature of the breach against the Severity Impact Rating Document (Appendix 2).

4.3 Reporting breaches

It is the applicant's responsibility to report all breaches, regardless of severity, to the Authority as soon as it is practicable. Breaches must be reported to the Authority within 48 hours after the breach has been identified. A completed *Information breach notification form* must be sent to the Authority's Research Officer at research@scsa.wa.edu.au within 48 hours of the breach occurring. Failure to do so will result in a breach of the applicant's information disclosure contract.

Following contact regarding an incident, the Research Officer or other such individual as deemed appropriate by the Authority will liaise with the applicant and inform them of any further actions he/she will need to take regarding the breach. Depending on the nature of the breach, possible consequences of breaches are as follows:

- increased monitoring of the project by the Authority
- amendments to the parameters of the Authority's approval
- suspension or cancellation of the Authority's approval
- exclusion of individuals responsible for the breach from future access to information from the Authority either for a fixed period of time or indefinitely

- reporting of individuals responsible for the breach to their employer, an external agent or statutory authority
- reporting allegations of criminal conduct to the police.

Depending on the nature and severity of the breach, civil or criminal penalties may be imposed.

Applicants are also required to inform individuals affected by a breach where known. A statement informing affected individuals must include the following:

- a description of the breach
- the information involved in the breach
- what steps the applicant recommends individuals take in response to the breach.

The Research Officer must inform the Authority's executive management of all actual and potential breaches as soon as practicable. In addition to this, the Research Officer must monitor the progress of the breach by maintaining communication with the applicant or the individual who discovered the breach. The Authority's executive management, with advice from the Authority Board, will determine the appropriate course of follow-up action(s) depending on the nature and severity of a breach.

The Research Officer must prepare a briefing note to the Authority Board outlining the situation, cause and resolution of a breach. In the event of a severe breach, the Research Officer may need to prepare a briefing note to the Director General and/or the Minister providing information about the breach.

5. Principles for reporting and accountability

The Authority Board may revoke an applicant's access to student information for non-compliance with the Authority's reporting and accountability principles. Non-compliance with the principles listed in the following sub-paragraphs may be regarded as non-compliance with an applicant's *Agreement for the disclosure of information*.

5.1 Principles for monitoring research projects

Applicants are required to provide the Authority with updates on the progress of their research projects, detailing how they have used the information received from the Authority in the *Annual report form* made available by the Authority.

Reports shall document the development and progress of the relevant research project, including reporting fields for how an applicant has used the information obtained from the Authority in their project. The Authority will stipulate content requirements for reporting in the information disclosure contract.

Continuing access to the student information obtained from the Authority is contingent on the timely completion and submission of reports. Applicants are required to submit reports by the due date determined by the Authority.

5.2 Principles for communication of research findings

The information obtained from the Authority used in reports and/or publications must be de-identified and must not allow for the identification of specific individuals, schools or school systems and sector.

5.3 Principles for auditing successful applications

The Authority may carry out audits of successful applications. To support auditing, successful applicants may receive requests from the Authority for the following:

- confirmation of approved users of student information provided by the Authority
- random inspections of research information and annual report forms
- audit of information security arrangements
- audit of access to information
- applicant responses to queries, complaints, or other questions related to the conduct of research, where student information provided by the Authority is used.

Applicants are required to comply with the Authority's requests. The Authority can revoke an applicant's access to information in the event of an applicant's non-compliance.

As a condition of receipt of student information from the Authority, applicants are required to inform the Authority of changes to the parameters in which a project is being conducted.

In the event of a change in circumstances that impacts the conduct of a given research project, the Authority Board may withdraw its approval for an application. In these circumstances, the Authority will inform the applicant of their withdrawal in writing and recommend that the applicant take all necessary steps in accordance with the approved information disposal procedures.

5.4 Principles for information disposal at project completion

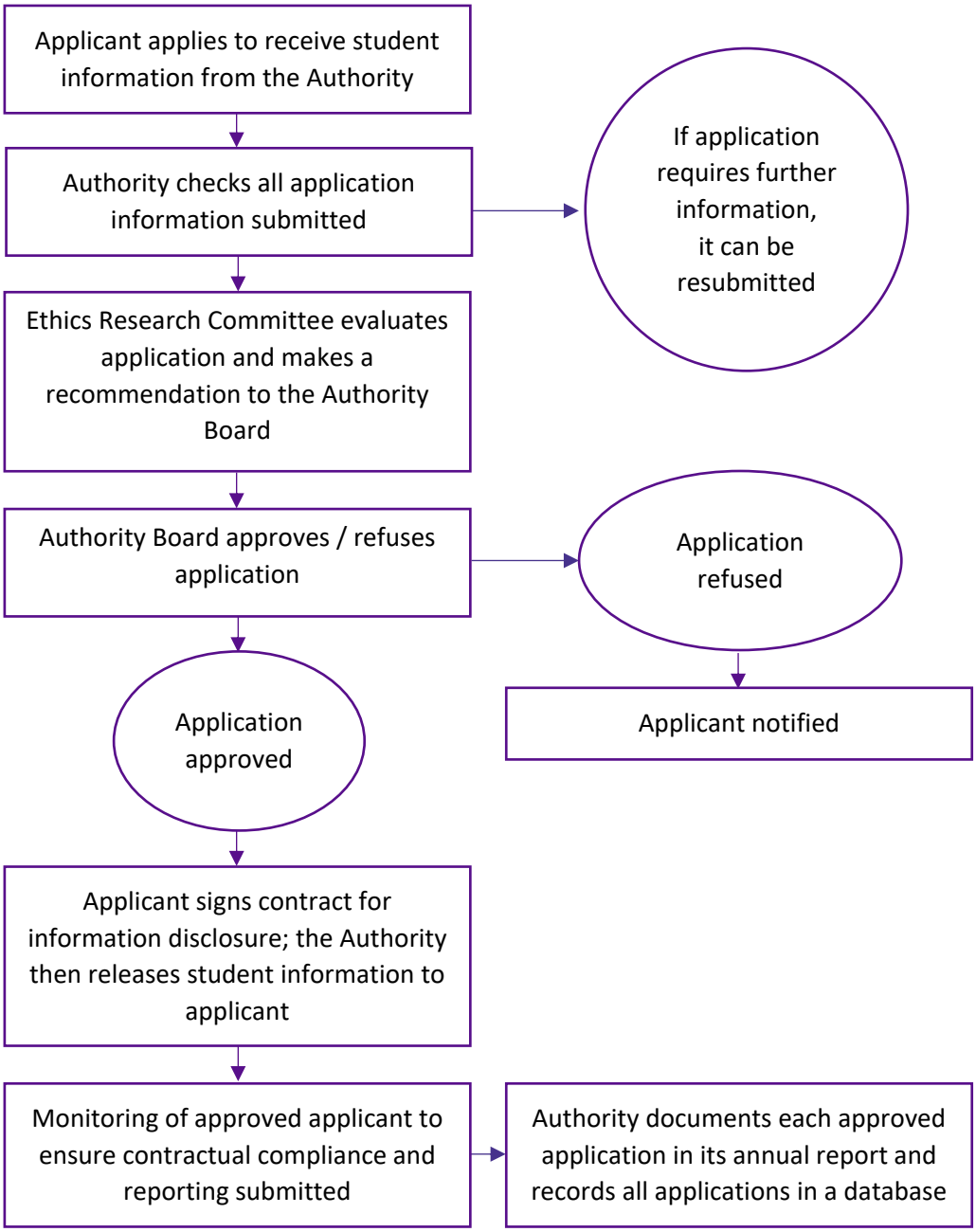
An applicant may only retain information obtained from the Authority for the period approved. The Authority must ensure that the procedures detailed in an applicant's disposal plan approved by the Authority are adhered to. The applicant must also submit a completed *Information disposal acknowledgement form* and a final *Annual report form* to the Authority at the conclusion of the research project.

The Authority will establish and maintain a register of records of information disposed of for future reference. The register will be updated when records are destroyed by an applicant. The register must also capture details of each record that is destroyed, as well as relevant information that pertains to the research application that the records are applicable to.

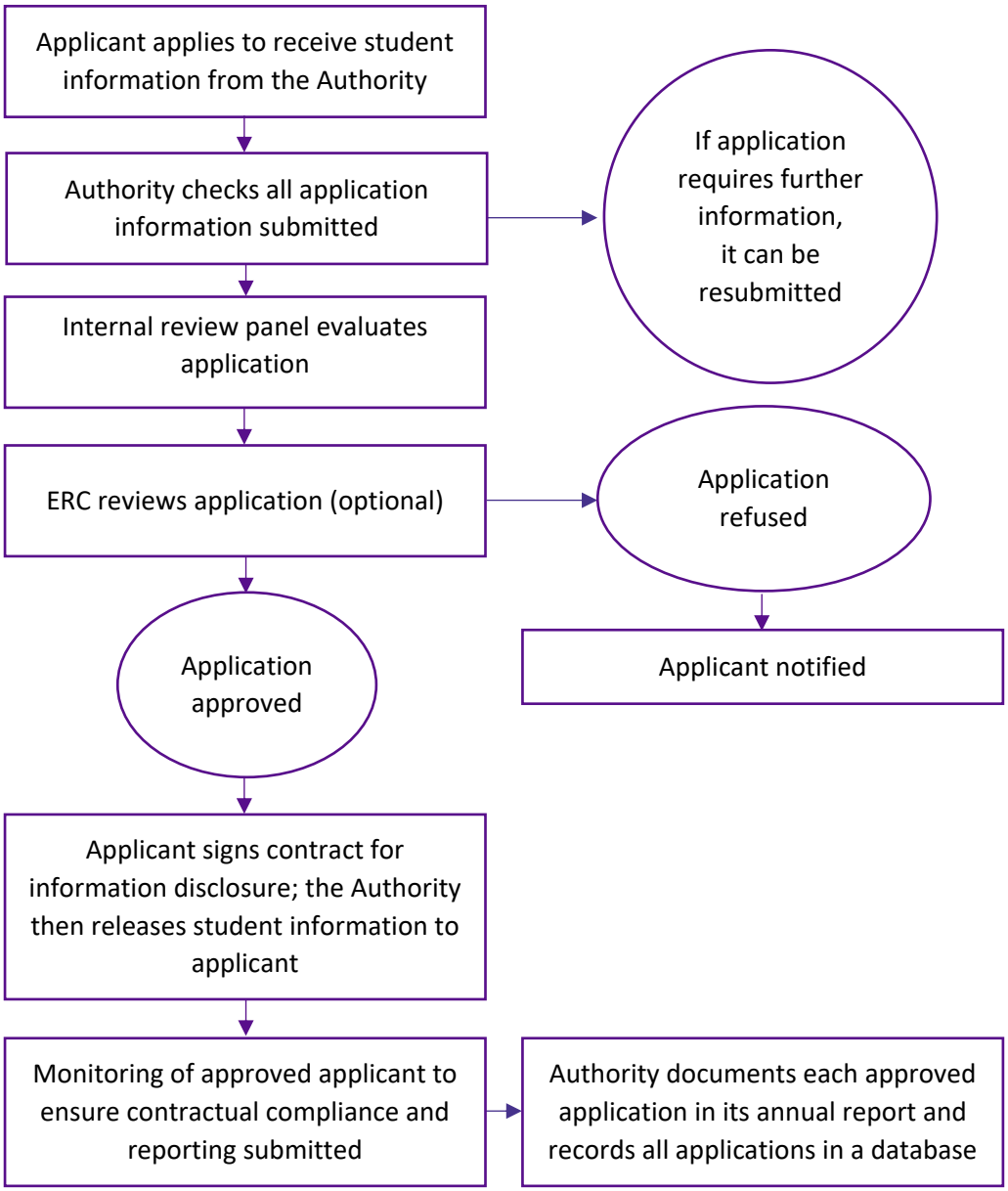
When a project is completed, a write-up that details the aims, findings and outcomes of a given research project must be submitted to the Authority.

6. Appendix 1: Approval process for information requests

Application process flowchart (identified information)



Application process flowchart (de-identified information)



7. Appendix 2: Severity Impact Rating Document

	Risk rating				
Consequence category	**1 Insignificant**	**2 Minor**	**3 Moderate**	**4 Major**	**5 Catastrophic**
Reputation and image	Unsubstantiated, low impact, low profile or no news item	Substantiated, low impact, low news profile	Substantiated, public awareness, moderate impact, moderate news profile (one-off incident)	Substantiated, public embarrassment, high impact, high news profile, third party actions (multiple and sustained impacts)	Substantiated, public embarrassment, very high multiple impacts (short term), sustained long term damage, high widespread multiple news profile, third party actions
Research participant	Risks that bring no real negative consequences or pose no significant threat to the wellbeing of the participant	Risks that have a small potential for negative consequences but will not have a significantly negative impact to the wellbeing of the participant	Risks that could potentially bring negative consequences, posing a moderate threat to the wellbeing of the participant	Risks with substantial negative consequences that will seriously affect the wellbeing of the participants	Risks with extreme negative consequences for the wellbeing of participants
Aboriginal and Torres Strait Islander cultural and community wellbeing	Risks that bring no real negative consequences or pose no significant threat to Aboriginal and Torres Strait Islander cultural and community wellbeing	Risks that have a small potential for negative consequences but will not have a significantly negative impact on Aboriginal and Torres Strait Islander cultural and community wellbeing	Risks that could potentially bring negative consequences, posing a moderate threat to Aboriginal and Torres Strait Islander cultural and community wellbeing	Risks with substantial negative consequences that will seriously affect Aboriginal and Torres Strait Islander cultural and community wellbeing	Risks with extreme negative consequences for Aboriginal and Torres Strait Islander cultural and community wellbeing