Secretary’s Guidelines

on the Victorian Student Number

Contents

Contents

[Version history 4](#_Toc135149154)

[Commencement 4](#_Toc135149155)

[Introduction 5](#_Toc135149156)

[Background 5](#_Toc135149157)

[The Victorian Student Number 5](#_Toc135149158)

[The Victorian Student Register 6](#_Toc135149159)

[Purpose of the Guidelines 7](#_Toc135149160)

[Status and compliance with the Guidelines 7](#_Toc135149161)

[Role of the Secretary and delegates 7](#_Toc135149162)

[Students and parents accessing the VSN 8](#_Toc135149163)

[Guidelines 8](#_Toc135149164)

[Authorised users 8](#_Toc135149165)

[Purposes for accessing, using and disclosing the VSN and related information 9](#_Toc135149166)

[Application process for authorisation 10](#_Toc135149167)

[Consideration of applications 11](#_Toc135149168)

[Relevant considerations when assessing an application for authorisation 11](#_Toc135149169)

[Notification of the outcome of an application 12](#_Toc135149170)

[Types of persons, bodies or classes of persons or bodies who may be authorised 12](#_Toc135149171)

[Conditions 13](#_Toc135149172)

[Revoking an authorisation 14](#_Toc135149173)

[Process for revoking an authorisation 14](#_Toc135149174)

[Reporting requirements 15](#_Toc135149175)

[Privacy and information management 15](#_Toc135149176)

[Privacy 15](#_Toc135149177)

[Record collection, storage and destruction 16](#_Toc135149178)

[Information sharing 18](#_Toc135149179)

[Disclosure to third parties 18](#_Toc135149180)

[Data breaches 20](#_Toc135149181)

[Application of the Charter of Human Rights and Responsibilities Act 2006 20](#_Toc135149182)

[Other matters 21](#_Toc135149183)

[Sharing cross-sectoral education data 21](#_Toc135149184)

[Updating personal information stored in the VSR 21](#_Toc135149185)

[Review of these Guidelines 21](#_Toc135149186)

# Version history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Issued** | **Dates of Effect** | |
|  |  | **From:** | **To:** |
| 1 | 24 May 2023 | 24 May 2023\* | Current |

\*Subject to the commencement details below.

# Commencement

Authorised users (other than the Victorian Curriculum and Assessment Authority) who have been authorised under section 5.3A.9 of the Education and Training Reform Act 2006 on or before 24 May 2023, are required to comply with these Guidelines on and from 24 September 2023.

The Victorian Curriculum and Assessment Authority is required to comply with these Guidelines on and from 24 May 2023.

All other authorised users are required to comply with these Guidelines on and from the date they are authorised.

# Introduction

## Background

### The Victorian Student Number

1. A Victorian Student Number (VSN) is a randomly generated 9-digit number assigned to all Victorian students as a unique identifier. Every student under 25 years of age is given a VSN when they first enrol at a Victorian education or training provider. For most students, this occurs when they enrol at a school in Foundation level. However, a student who does not already have a VSN will be given one when enrolled at a Victorian education or training provider any time before they turn 25 years of age (for example, because they have relocated from interstate). Students keep the same VSN connected to their personal information when they change education or training providers in Victoria.
2. The legislation that establishes and governs the VSN and related information is in Part 5.3A of the *Education and Training Reform Act 2006* (the Act). These Guidelines are issued by the Secretary to the Department of Education (Secretary) under section 5.3A.10A(1) of the Act and should be read together with Part 5.3A.
3. The Act requires that every student under 25 years of age be given a VSN when they enrol at a Victorian education or training provider, or are registered by the Victorian Registration and Qualifications Authority (VRQA) for home schooling.[[1]](#footnote-2) This includes students who are enrolled at a:
4. Government school
5. Catholic school; or
6. Independent school.
7. VSNs are also provided to students under 25 years of age undertaking vocational education and training (VET) with a:
8. TAFE institute
9. registered training organisation (RTO); or
10. adult, community and further education (ACFE) provider that is funded by the ACFE Board.[[2]](#footnote-3)
11. When a student is enrolled at an education or training provider, or registered for home schooling by the VRQA, the provider or relevant authority must apply to the VCAA, as the delegate of the Secretary, to allocate the student a VSN or to verify the student’s VSN if they have already been allocated one.[[3]](#footnote-4) More information on the Secretary’s delegation of powers and functions related to the administration of the VSN can be found below at paragraph 16.
12. The VSN allows education and training providers to record and monitor the enrolment of students in Victoria, and to track students’ progress through their school age years and beyond, should they continue into VET. This enables students’ records to be accurately maintained, ensures education and training providers have appropriate levels of resourcing, and enables schools and support services to identify instances of disengagement from the school system while children remain of compulsory school age.
13. The VSN also provides the Department of Education (department), the Department of Jobs, Skills, Industry and Regions, education and training providers, and other relevant parties with a data set to conduct analysis and research that can inform operational and policy decisions to improve education and training at an individual provider level and for the whole system.

### The Victorian Student Register

1. The Victorian Student Register (VSR) is a secure database containing VSNs for enrolled Victorian students up to the age of 25, as well as additional ‘related information’[[4]](#footnote-5) for each student, including:
2. the student’s full name
3. the student’s date of birth
4. the student’s gender
5. the date on which the student is enrolled at an education or training provider or registered for home schooling by the VRQA
6. the date on which the student’s enrolment at an education or training provider or registration for home schooling is cancelled; and
7. the records of changes which have been made to data.
8. The VSR is managed by the [Victorian Curriculum and Assessment Authority (VCAA)](https://www.vcaa.vic.edu.au/Pages/HomePage.aspx) under delegated authority from the Secretary. The VCAA is a statutory authority primarily accountable to the Minister for Education, serving both government and non-government schools.
9. The VCAA manages a range of functions relating to the collection, maintenance and quality assurance of the VSN and related information within the VSR. These include:
10. maintaining the data integrity of the VSN and related information
11. managing applications for authorisation to access, use and disclose the VSN and related information; and
12. disclosing the VSN and related information to authorised users and other persons who have a right to access that information, such as students and their parents.
13. The VCAA also enables the VSN and related information to be entered manually by education and training providers, or to be sent and received automatically via systems used by education and training providers.

## Purpose of the Guidelines

1. The purpose of these Guidelines is to provide additional guidance and impose additional requirements regarding the VSN in relation to the following matters:[[5]](#footnote-6)
2. the process for applying for authorisation to access, use or disclose the VSN or related information
3. the matters to be considered in relation to authorising a person, body or class of persons or bodies to access, use or disclose the VSN or related information
4. the process for giving an authorisation and notification of the making of an authorisation
5. the types of persons, bodies or classes of persons or bodies who may be authorised to access, use or disclose the VSN or related information
6. the manner in which an authorised user may access, use or disclose the VSN or related information for permitted purposes
7. the processes for giving and revoking an authorisation
8. reporting requirements for authorised users in relation to the VSN and related information
9. information management, including the manner in which an authorised user may access, use or disclose the VSN or related information for a permitted purpose, and the storage and destruction of the VSN and related information; and
10. privacy and protection of students’ personal information.

## Status and compliance with the Guidelines

1. The Guidelines contain both mandatory requirements that must be followed, as well as guidance and information to assist authorised users and other interested parties to understand and comply with the restrictions and permitted uses for the access, use and disclosure of the VSN and related information.
2. Authorised users must comply with these Guidelines.[[6]](#footnote-7) An authorised user’s failure to comply may result in their authorisation being revoked in certain circumstances.
3. An authorised user may commit an offence if they access, use or disclose the VSN or related information other than in accordance with Division 3 of Part 5.3A of the Act.[[7]](#footnote-8) The maximum penalty for this offence is 30 penalty units (information on penalty unit values can be found [here](https://www.justice.vic.gov.au/justice-system/fines-and-penalties/penalties-and-values#:~:text=Penalty%20units%20determine%20the%20amount,the%20nearest%20dollar)%20is%20%24370.)). The offence does not apply to an authorised user that is a statutory authority and a failure to comply with the Guidelines does not constitute an offence against section 5.3A.10(1) of the Act.

## Role of the Secretary and delegates

1. The Secretary has delegated responsibility for making decisions regarding authorising a person or body to access, use and disclose the VSN and related information to the VCAA. As delegate of the Secretary, the VCAA must have regard to the Guidelines in relation to their exercise of any delegated powers or functions.
2. Despite the delegation of power, the Secretary can still exercise the power to authorise users in their own right, and the Secretary or delegate must have regard to these Guidelines when giving or revoking an authorisation.[[8]](#footnote-9)

## Students and parents accessing the VSN

1. Students and/or their parents may access a copy of that student’s information recorded in the VSR, which includes the VSN and related information.[[9]](#footnote-10) They do not need to apply to become an authorised user under these Guidelines to do so. Under the Act, a parent includes a guardian and every person who has parental responsibility for the child including parental responsibility under the *Family Law Act 1975* (Cth) and any person with whom a child normally or regularly resides.
2. To access their information, a student or their parent must either:
3. apply to the education or training provider at which a student is currently enrolled; or
4. apply directly to the VCAA via email at [vsr@education.vic.gov.au](mailto:vsr@education.vic.gov.au).
5. Where an application is made directly to the VCAA, this must include:
6. a student’s full name (as it appears on official identification documents) and date of birth
7. evidence of the student’s identity in the form of a copy of a primary identity document, such as a passport or birth certificate; and
8. if the applicant is a student’s parent, a copy of a primary identity document of the applicant and evidence of the applicant’s relationship to the student, such as a copy of a birth certificate or other document evidencing this.[[10]](#footnote-11)

# Guidelines

## Authorised users

1. The VCAA, as the Secretary’s delegate, may authorise a person, body, or class of persons or bodies, to access, use or disclose the VSN and related information for one or more of the permitted purposes set out in the Act.[[11]](#footnote-12) The permitted purposes are described in more detail below at paragraph 24.
2. As the VSN and related information contains personal information, the Secretary and the VCAA, as the delegate responsible for considering requests for authorisation, will tightly control which persons or bodies should be authorised users.
3. If the VCAA decides to give an authorisation, this will:
4. be issued in writing[[12]](#footnote-13)
5. set out the purpose or purposes for which the authorised user may access, use or disclose the VSN and related information[[13]](#footnote-14) (see ‘Purposes’ section below); and
6. list any conditions that apply to the authorisation[[14]](#footnote-15) (see ‘Conditions’ section at paragraph 38).

### Purposes for accessing, using and disclosing the VSN and related information

1. Authorised users may only be authorised to access, use or disclose the VSN and related information for a purpose specified in the Act.[[15]](#footnote-16) These ‘permitted purposes’ are:
2. monitoring and ensuring student enrolment and attendance
3. ensuring education or training providers and students receive appropriate resources
4. statistical purposes relating to education or training
5. research purposes relating to education or training
6. ensuring students’ educational records are accurately maintained
7. as required or authorised by or under law
8. a purpose prescribed in the Education and Training Reform Regulations 2017; and
9. a purpose specified in a Ministerial Order.

Common examples of access, use and disclosure that may represent permitted purposes

|  |  |
| --- | --- |
| Purpose | Example |
| a) monitoring and ensuring student enrolment and attendance | The department’s annual monitoring of student enrolment details enables the identification of students at risk of leaving education and training early. It is also used to drive programs and policies which aim to keep students engaged in education and training. |
| b) ensuring education or training providers and students receive appropriate resources | Schools request the VSN and related information from the VSR to:   * ensure their enrolment data is accurate * support reporting to the Victorian government for planning purposes; and * calculate indicative funding for schools. |
| c) statistical purposes relating to education or training | The VSR provides enrolment numbers and student demographics to help organisations understand education demand. |
| d) research purposes relating to education or training | Social researchers and higher education providers may use the VSN and related information to establish links between education and training and other social metrics of wellbeing. |
| e) ensuring students’ educational records are accurately maintained | The VSN is used to verify student identity for welfare and data integrity. |
| f) as required or authorised by or under law | Law enforcement agencies, such as Victoria Police or the Australian Federal Police, may require the production of information stored in VSR for the purposes of legal proceedings, investigations or inquiries. This may be done, for example, to establish historical enrolment and attendance of a student at an education or training provider for one of these purposes.  An example of disclosing the VSN or related information as authorised by law, is a disclosure under the Child Information Sharing Scheme in Part 6A of the *Child Wellbeing and Safety Act 2005.* See the‘Child wellbeing and safety and family violence’ section of these Guidelines for more information.  More information on this purpose can be found in the ‘Privacy and protections’ section of these Guidelines. |

### Application process for authorisation

1. A person or body seeking to become an authorised user must submit an application to the VCAA. When preparing an application for authorisation, prospective applicants should note that:
2. applications must be submitted in writing using the [application form](https://www.vcaa.vic.edu.au/administration/schooladministration/student-numbers/Pages/VSNDataRequests.aspx#AppForm)
3. applications must be submitted using the method specified in the form
4. as part of their application, an applicant must:
   1. provide the information requested in the form, including relevant supporting documentation
   2. list the reason or reasons for which the applicant seeks to access, use and/or disclose the VSN and related information
   3. list the permitted purpose or purposes under which the applicant believes each reason falls, as listed above at paragraph 24; and
   4. list any third parties to whom they may need to disclose the VSN and related information, the reason (linked to a permitted purpose) they may disclose it and how they will manage privacy and data security in making a disclosure to a third party.
5. the VCAA may request further information in relation to the application.
6. Prospective applicants may contact the VCAA to seek assistance with or additional information about the application process. Before contacting the VCAA with queries in relation to applications, prospective applicants should read these Guidelines, Part 5.3A of the Act, and the application form.
7. Existing authorised users seeking to update their authorisation (e.g., to permit the sharing of the VSN and related information to a new third party not already allowed in their current authorisations) should contact the VCAA to seek assistance.

### Consideration of applications

1. Applications are considered on a case-by-case basis with reference to the Act, these Guidelines, and other relevant policies and procedures.
2. If further information is required in relation to an application, the VCAA will contact applicants in writing to seek that information.
3. The VCAA will aim to make a decision on whether or not to grant authorisation within 10 business days. This timeframe may be extended at the VCAA’s discretion, including where an application is incomplete, complex, or further information is required. The VCAA will inform the applicant in writing if a decision will not be made within 10 business days.

### Relevant considerations when assessing an application for authorisation

1. When making a decision to grant or refuse an application for authorisation, the VCAA must consider:
2. whether a person, body or class of persons or bodies is suitable for authorisation
3. whether the reason for which access, use or disclosure is sought is a permitted purpose under the Act
4. how the VSN and related information will be accessed, used, disclosed or destroyed
5. any privacy implications; and
6. any human rights implications.
7. In assessing whether a person, body or class of persons or bodies is suitable for authorisation, factors that the VCAA will consider include, but are not limited to:
8. what security and other arrangements the proposed user will put in place to protect the VSN and related information from unauthorised use, access, or disclosure
9. the information security management processes the proposed user currently has in place, including:
   1. an information security risk management framework
   2. incident management processes (including disaster recovery processes and plans)
   3. personnel, ICT and physical security controls
   4. how the proposed user manages information security with any third parties that it provides information to; and
   5. details of compliance with any standards applicable to information security management (i.e.: ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection - Information security management systems – Requirements;the Victorian Protective Data Security Standards and Framework; the cyber security guidelines within the Information Security Manual by the Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD)).
10. whether the person, body or class of persons or bodies will be able to meet their privacy obligations under the legislation that applies to them or will apply to them if they are authorised
11. the extent to which the proposed user will utilise secure, and automated, systems for the transfer of data in lieu of less secure and ad hoc methods (such as email)
12. the results of any Privacy Impact Assessment, Data Security Assessment, or relevant security audit
13. for individuals: if the individual is fit and proper to hold an authorisation, including whether they have a criminal record, a history of misusing information, or have been the subject of any misconduct proceedings or adverse findings, including under the *Worker Screening Act 2020*
14. for bodies: how the body will ensure that only fit and proper individuals within the organisation will have access to the VSN and related information
15. whether the applicant has previously had their authorisation suspended or revoked or been subject to other relevant adverse findings
16. whether the information being sought can be obtained elsewhere
17. whether the applicant can meet the requirements that would apply to them in Part 5.3A of the Act and these Guidelines; and
18. any other matters that it deems relevant.

### Notification of the outcome of an application

1. When a decision is made in relation to an application, the VCAA will:
2. inform the applicant in writing of the outcome of the application
3. confirm the date that any authorisation takes effect
4. inform the applicant in writing of any conditions that apply to their authorisation; and
5. provide a copy or relevant extract of any authorisation to the authorised user.
6. If an authorisation is granted, authorised users will then receive the data requested in a manner agreed with the VCAA.
7. Data on the number of authorisations granted and the permitted purposes for which authorised users may access, use or disclose the VSN and related information may be included in reports and published on the websites of the department or the VCAA.

### Types of persons, bodies or classes of persons or bodies who may be authorised

1. Existing users and classes of users that have been authorised before 24 May 2023 remain authorised users under the Act until their authorisation is revoked.[[16]](#footnote-17) Users authorised before 24 May 2023 include:
2. the VCAA
3. the VRQA
4. any education or training provider (as defined in section 5.3A.1 of the Act)
5. an employee of the Catholic Education Commission or of a Catholic education agency; and
6. an employee of the department.
7. Existing users and classes of users that have been authorised before 24 May 2023 are also subject to the requirements of the Act and these Guidelines. This means that requests to access, use and disclose the VSN and related information from these users must align with the purposes in section 5.3A.9(2) of the Act and described above at paragraph 24. These authorised users can also have their authorisations revoked.

**A variety of groups can seek to access, use and disclose the VSN and related information**

* Research institutes and universities seeking to conduct research for a permitted purposes may seek to become authorised users.
* Law enforcement bodies, such as police or courts, may seek to access VSN information during investigations or legal proceedings, including, for example, to understand where a child attends school.
* Third party contractors, such as IT contractors, doing work for an authorised user that requires them to access VSN information may seek authorisation. This includes contractors supporting schools to manage their student management software.

### Conditions

1. The VCAA may impose conditions on the authorisation given to an authorised user.[[17]](#footnote-18)
2. Conditions on an authorisation may include, but are not limited to:
3. requirements or limitations in relation to how information is collected, stored, disclosed, or destroyed
4. a time limit on the authorisation
5. requirements for a Privacy Impact Assessment and/ or Data Security Assessment to be undertaken
6. requirements to undertake independent cyber security and privacy audits at regular intervals, or upon request by the Secretary; and
7. any other conditions that the VCAA considers necessary.
8. Examples of common conditions that may be imposed include conditions that:
9. limit the duration of an authorisation to the lifetime of a project, and that require the destruction of all VSNs and related information after a project ends
10. limit the authorisation to disclose the VSN or related information to certain specified persons or classes of persons (and do not permit disclosure to the world at large, or on-forwarding to other parties) depending on the reasons for and purposes set out in the authorisation; and
11. the authorised user seek the consent of a person or body before accessing or publishing certain information, such as where a request is made for information that may be used to make comparisons of performance across educational sectors.
12. Any conditions attached to an authorisation will be included in an authorised user’s instrument of authorisation.
13. If, after viewing the instrument, an authorised user is unsure about whether conditions apply, the meaning or effect of a condition, or whether the conditions of another authorised user’s authorisation allow the disclosure of the VSN and related information to them, they may contact the VCAA at [vsr@education.vic.gov.au](mailto:vsr@education.vic.gov.au).

### Revoking an authorisation

1. The Secretary, or the VCAA, may revoke an authorisation at any time.[[18]](#footnote-19) When revoking an authorisation, the VCAA must have regard to these Guidelines.[[19]](#footnote-20)
2. An authorisation may be revoked when the VCAA considers it is no longer required or appropriate or where the reason for the authorisation no longer exists, such as where the body no longer exists (for example, where a school or RTO closes) or a project to develop an IT system for use by a school ends.
3. Other circumstances in which an authorisation may be revoked include:
4. non-compliance with the Act (including any privacy legislation applying by virtue of the Act), the Guidelines, or an authorised user’s authorisation
5. misconduct, for example, where the VCAA considers that an authorised user has used, or is likely to use, the VSN or related information improperly or has otherwise engaged in conduct that would lead the VCAA to form the view that it is no longer appropriate for the authorised user to have access to the VSN or related information
6. where the authorised user is no longer suitable to be an authorised user; and
7. for any other reason determined by the VCAA.

### Process for revoking an authorisation

1. When proposing to revoke an authorisation, the VCAA must:
2. notify the authorised user in writing of the proposal to revoke their authorisation
3. provide the authorised user subject to the proposed revocation the opportunity to provide information as to why their authorisation should not be revoked (usually 10 business days)
4. take any relevant information provided into account before making a final decision; and
5. provide the authorised user the decision and reasons for the decision in writing.
6. Where the VCAA proposes to revoke an authorisation, it may suspend an authorisation during the notification process, pending a final decision being made in relation to the proposed revocation. This may include suspending access to the VSN and related information during this process, including by suspending access to the VSN and related information by any relevant student management system (SMS).
7. If a decision is made to revoke an authorised user’s authorisation:
   1. any systems access to the VSN and related information will be rescinded within 24 hours of the revocation decision, including any access provided to a SMS of the authorised user; and
   2. the formerly authorised user may be required to sign a statutory declaration that it has destroyed any copies of the VSN or related information it, and any of its contractors, had access to.
8. At regular intervals the VCAA will audit the user access arrangements in place for the VSN and related information to ensure that it matches the current list of authorised users and any SMS the current authorised users rely on.
9. The VCAA may also seek assurances from authorised users, at regular intervals, that the authorised user audits the access they provide to employees for any SMS, and removes access when no longer required.

## Reporting requirements

1. The VCAA is required to report to the Secretary and department, and the Minister, each year on delegated VSN functions, including the number of applications for authorisations, the number of authorisations granted, and the number of disclosures of the VSN and related information approved by the VCAA.

## Privacy and information management

### Privacy

1. Some authorised users may already be subject to either the *Privacy and Data Protection Act* *2014* (Vic) (Victorian Privacy and Data Protection Act) or the *Privacy Act 1988* (Cth) (Commonwealth Privacy Act) (or both). These authorised users are already required to comply with those laws, including the privacy principles in those laws, as they apply to the collection, use, disclosure, storage, and destruction of the VSN and related information. The agencies and organisations subject to these Acts are listed below at paragraphs 54 and 55.
2. An authorised user who is not already required to comply with either the Victorian Privacy and Data Protection Act or the Commonwealth Privacy Act (for example, because they are not an agency or organisation listed at paragraphs 52 and 53), are deemed to be subject to the Victorian Privacy and Data Protection Act, including the Information Privacy Principles (IPPs), in relation to their handling of personal information or unique identifiers under Part 5.3A. These authorised users must comply with the Victorian Privacy and Data Protection Act as if they were an organisation within the meaning of that Act.[[20]](#footnote-21)
3. The Victorian Privacy and Data Protection Act applies to organisations as defined in that Act,[[21]](#footnote-22) including:
4. public sector agencies
5. bodies established or appointed for a public purpose by or under an Act or by the Governor in Council or a Minister
6. a person holding an office or position established by or under an Act or appointed by the Governor in Council or a Minister
7. a court or tribunal
8. Victoria Police; and
9. a contracted service provider in relation to its provision of services under a State contract that specifies it is bound by the IPPs.
10. The Commonwealth Privacy Act applies to agencies and organisations as defined in that Act, including:
11. a Commonwealth Minister
12. a Commonwealth Department
13. a body or tribunal established or appointed for a public purpose by or under a Commonwealth law
14. a body established or appointed by the Governor-General or a Commonwealth Minister
15. a person holding or performing the duties of an office established by or under, or an appointment made, under a Commonwealth law
16. a federal court
17. the Australian Federal Police; and
18. an individual, body corporate, partnership, other unincorporated association or trust that is not a small business operator or a registered political party.[[22]](#footnote-23)
19. If a person or body is unsure whether they are required to comply with the Victorian Privacy and Data Protection Act or the Commonwealth Privacy Act, they should enquire with the Office of the Victorian Information Commissioner (OVIC) and the Office of the Australian Information Commissioner (OAIC) prior to applying for authorisation.
20. The VCAA is subject to the Victorian Privacy and Data Protection Act as an organisation under that Act.[[23]](#footnote-24) As a result, the VCAA is required to act consistently with the IPPs in respect of personal information collected, held, managed, used, disclosed or transferred by it.

### Record collection, storage and destruction

1. The information stored in the VSR is collected from individual students upon enrolment by the education and training provider they are enrolled with, and by the VRQA upon registration for home schooling.
2. All information in the VSR must be stored and managed in accordance with the relevant retention and disposal authority made under the *Public Records Act 1973* (Public Records Act), in addition to any relevant Standards published under the Public Records Act by the Public Record Office Victoria.
3. Authorised users are required to safeguard and protect the VSN and related information against the destruction, loss, unauthorised access to and disclosure of the VSN and related information in the possession, power or control of the authorised user or any personnel.[[24]](#footnote-25)
4. Authorised users are required to have robust information security management processes in place to safeguard the VSN and related information, including:
5. an information security risk management framework
6. incident management processes (including disaster recovery processes and plans)
7. personnel, ICT and physical security controls; and
8. processes to manage information security with any third parties that it provides information to.
9. All authorised users and any personnel must:
10. if applicable, ensure that the information system of the authorised user or any personnel is maintained and updated in accordance with recommendations from the provider or providers of the operating system, database, anti-virus, anti-malware or other software and hardware components utilised in the information system[[25]](#footnote-26)
11. operate and maintain robust processes for granting and revoking privileged access to any systems used to store or process the VSN and related information
12. maintain a physically secure environment for the storage of the VSN and related information
13. make and maintain regular and secure backups of the VSN and related information
14. store and maintain the VSN and related information (including backup storage) at sites located in Australia; and
15. not permit the VSN or related information to be made available, transferred or disclosed to any recipient located outside Australia, except with the prior written consent of the department.
16. An authorised user must not enter into a contract with any third party contractor for the provision of services to the authorised user in respect of the VSN and related information collected, held, used, managed, disclosed or transferred by or on behalf of the authorised user, unless: the terms and conditions of the contract require the third party contractor to comply with the privacy and information management requirements in these Guidelines as though the contractor were the authorised user.
17. Where authorisation has been revoked, the Secretary or the VCAA may direct that VSN and related information be securely destroyed. The Secretary or the VCAA may seek evidence or assurances, including in the form of a statutory declaration from the authorised user and any third party to whom the authorised user has disclosed, that destruction of VSN and related information has occurred.

### Information sharing

1. Certain public authorities may submit requests to the VCAA or authorised users to access, use or disclose the VSN and related information to support students’ welfare under established information sharing schemes, including the Child Information Sharing Scheme, the Family Violence Information Sharing Scheme, or under the *Terrorism (Community Protection) Act 2003* (Community Protection Act). Where sharing that information with a relevant public authority is authorised under legislation, these Guidelines do not require that authority to become an authorised user under the Act.

**Child wellbeing and safety and family violence**

1. The Child Information Sharing Scheme,[[26]](#footnote-27) the Family Violence Information Sharing Scheme,[[27]](#footnote-28) and the Community Protection Act allow specified organisations to access the VSN and related information, with the aims of supporting child wellbeing and safety, assessing and protecting against family violence, and countering violent extremism.
2. Where an authorised user is also prescribed as an information sharing entity (ISE) for the purpose of these schemes under the *Child Wellbeing and Safety Act 2005*, the *Family Violence Protection Act 2008* or the Community Protection Act, they may be empowered to access, use or disclose the VSN and related information both:
3. in their capacity as an ISE under those laws; and/or
4. as an authorised user under the Act and these Guidelines.
5. ISEs should have regard to the capacity in which they are accessing, using or disclosing the VSN or related information, and the legal basis underpinning this. This will determine what requirements apply to their access, use or disclosure of the VSN and related information. If an ISE is accessing, using or disclosing the VSN or related information for a purpose under the *Child Wellbeing and Safety Act 2005*, the *Family Violence Protection Act 2008* or the Community Protection Act, the ISE must abide by those obligations. If they are accessing, using or disclosing the VSN or related information under the Act, the Act and these Guidelines apply.

### Disclosure to third parties

1. Authorised users must only disclose the VSN and related information to third parties where their authorisation allows them to do so, having regard to the purpose or purposes for which the authorisation was given and any conditions applying to the authorisation.
2. For example, if an authorisation is granted for the purposes of maintaining accurate records and monitoring enrolment or attendance and states that the VSN and related information may be disclosed to certain third parties, then it allows disclosure only to those third parties. The authorised user is not authorised to disclose the information to other third parties outside of the scope of the authorisation, even where it meets the purpose set out in the authorisation.
3. Authorised users should consider the need for any disclosure to third parties prior to applying for authorisation and provide that information to the VCAA to ensure that the authorisation is fit for purpose and has adequate scope to enable the permitted purposes to be achieved.

**Contractors and IT systems**

1. Many education and training providers use third parties to manage their SMS or IT system.
2. Before sharing the VSN and related information, education and training providers must ensure that the contract under which a third party is engaged includes obligations to comply with relevant privacy laws, obligations under these Guidelines, and to notify the authorised user of all data breaches and take appropriate actions in such circumstances. Authorised users should also ensure contractors who have access to the VSN and related information understand their obligations under the Act and these Guidelines.
3. Education and training providers can connect directly to the VSR to enrol students, either manually or automatically via an SMS. Education and training providers are responsible for referring any SMS supplier they seek to engage to the VCAA. The VCAA will then undertake systems testing to determine whether the SMS contains adequate privacy and security features to ensure secure and compliant connections to the VSR. As part of these tests, the prospective SMS supplier may be required to respond in writing to questions from the VCAA.
4. At the conclusion of the testing process, the VCAA will notify the supplier and the education or training provider in writing whether the supplier is approved to connect to the VSR on the provider’s behalf via the SMS. Further information about connecting to the VSR may be made available throughout the authorisation process and upon request to the VCAA.

**Other third-party disclosures**

1. An authorised user may disclose the VSN and related information to another authorised user for a permitted purpose under the Act if the conditions of both users’ authorisation permit this.
2. Authorised users may also be required to disclose the VSN and related information that they have access to if required by law. This may include, for example, a third party exercising a legal power to require or compel the production of information. Bodies with such powers include law enforcement agencies such as Victoria Police or the Australian Federal Police, tribunals, courts, and Royal Commissions, which may seek the VSN and/or related information as part of an investigation, inquiry or litigation.
3. For example, the department or a school could disclose the VSN or related information in response to a warrant issued by a magistrate or a court order (such as a summons from the Children’s Court). Further, the VSN or related information could be disclosed in response to a request for information from a magistrate during the course of proceedings, provided that the request comes from the magistrate acting as the Court.
4. A lawyer who is representing a child, or a child’s parent, may also be able to access the VSN or related information. This is because the relationship between a lawyer and client is one of principal and agent, and a lawyer may have the power to act on their client’s behalf and may do so for the purposes of seeking access to a student’s VSN and related information under section 5.3A.12 of the Act and these Guidelines. To establish whether a lawyer is acting on behalf of a student or parent behalf, an authorised user should request confirmation in writing that the lawyer has instructions to act on their behalf and to request the information under section 5.3A.12 of the Act.

### Data breaches

1. A breach may arise as a result of acts or omissions by an authorised user, or by a third party to whom the authorised user has disclosed the VSN and related information, such as an IT contractor engaged by the authorised user to build or maintain an SMS.
2. Some authorised users and their personnel have obligations in relation to data breaches under Standard 9 of the Victorian Protective Data Security Standards V2.0 (VPDSS)**.**[[28]](#footnote-29) Element E 9.010 of the Implementation Guidance to the VPDSS provides that, in accordance with the OVIC Information Security Incident Notification Scheme, relevant organisations should notify OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level of 2 (limited) or higher. Further information on steps to be taken under the OVIC Information Security Incident Notification Scheme in relation to data breaches, and which organisations have obligations under the Scheme, can be found here.
3. Authorised users covered by the Commonwealth Privacy Act will have obligations under the Notifiable Data Breaches scheme within that Act. The scheme requires that affected individuals and OAIC are notified if there has been a data breach involving personal information, and which is likely to result in serious harm.[[29]](#footnote-30) More information on that scheme can be found [here](https://www.oaic.gov.au/privacy/notifiable-data-breaches).
4. If there is a data breach in relation to the VSN or related information, the relevant authorised user or person to whom the VSN or related information has been disclosed, outside of the department or the VCAA, must notify any data breach they become aware of to the VCAA as soon as reasonably practicable at vsr@education.vic.gov.au. The authorised user must take steps to contain, investigate and remediate the data breach.
5. The VCAA and the department have protocols in place in relation to data breaches, which involve the relevant information security and privacy units and privacy officers managing the incidents. If the VCAA is notified of a data breach by an authorised user or person to whom the VSN or related information has been disclosed, the VCAA will inform the department’s Privacy Unit and collaborate with them to address the breach. Authorised users must use their best endeavours to comply with any directions given by the VCAA in relation to the data breach and to support the VCAA in understanding and adequately dealing with the breach, including to ensure the security of any information as soon as possible.
6. Most data breaches will also be subject to the jurisdiction of OVIC under the Victorian Privacy and Data Protection Act. OVIC may undertake investigations, issue compliance notices with potential penalties and prepare public reports. Agencies and organisations subject to the Commonwealth Privacy Act will be subject to the jurisdiction of OAIC.

### Application of the Charter of Human Rights and Responsibilities Act 2006

1. Public authorities such as the VCAA and the department must have regard to the *Charter of Human Rights and Responsibilities Act 2006* (Charter), including when making decisions. It is unlawful for a public authority to act in a way that is incompatible with a human right or, in making a decision, to fail to give proper consideration to a relevant human right.[[30]](#footnote-31)

## Other matters

### Sharing cross-sectoral education data

1. The VSR holds information about student records from across different Victorian education sectors. If there is a request for statistical information which draws on cross-sectoral data, the VCAA may impose a condition on an authorisation to require the requestor to seek permission from leaders in those sectors to access this data. This is out of respect for the sensitivity of direct or inadvertent measuring of school or sector performance across sectors.

### Updating personal information stored in the VSR

1. There may be circumstances in which the personal information stored in the VSR needs to be updated, for example if a student changes their name. As a key purpose of the VSN and related information is to track student progress, and data integrity is key to this process, the name on the VSR will be a student’s full name, as it appears on official identification documents such as a birth certificate or passport. Other names, such as preferred and anglicised names, will only be included if supported by an official identification document. Pseudonyms are not required on the VSR as there are strict restrictions on who can the access, use and disclose of the information and stringent requirements on the information security and privacy protections that must be in place in order for access to be granted.
2. For students who are enrolled at an education and training provider, all requests to change personal information stored in the VSR must be made through their provider. The student must provide the relevant information to be updated, and any required documentation, to the provider. The provider must provide this information to the VCAA, who will then update the information if all requirements are met.
3. For students who are registered for home schooling, all requests to change personal information stored in the VSR must be made through the VRQA. The student must provide the relevant information to be updated, and any required documentation, to the VRQA. The VRQA must provide this information to the VCAA, who will then update the information.
4. For information on how to update personal information stored in the VSR, contact the VCAA.

## Review of these Guidelines

1. These Guidelines will be reviewed every 3 years to ensure the content is up to date and current with relevant policies and processes. The department will consult the VCAA on any necessary updates to the Guidelines. The Secretary or delegate may review the Guidelines and issue amended Guidelines at any time, as they consider necessary.

1. Sections 5.3A.2, 5.3A.3 and 5.3A.5 of the Act. [↑](#footnote-ref-2)
2. See definition of ‘education or training provider’ in section 5.3A.1 of the Act. [↑](#footnote-ref-3)
3. Sections 5.3A.3(1) and (2) of the Act. [↑](#footnote-ref-4)
4. See definition of ‘related information’ in section 5.3A.1 of the Act. [↑](#footnote-ref-5)
5. Section 5.3A.10A of the Act. [↑](#footnote-ref-6)
6. Section 5.3A.10B of the Act. [↑](#footnote-ref-7)
7. Section 5.3A.10 of the Act. [↑](#footnote-ref-8)
8. Section 5.3A.9A of the Act. [↑](#footnote-ref-9)
9. Section 5.3A.11 of the Act. [↑](#footnote-ref-10)
10. Section 5.3A.11 of the Act. [↑](#footnote-ref-11)
11. Section 5.3A.9 of the Act. [↑](#footnote-ref-12)
12. Section 5.3A.9(1) of the Act. [↑](#footnote-ref-13)
13. Section 5.3A.9(2) of the Act. [↑](#footnote-ref-14)
14. Section 5.3A.9(3) of the Act. [↑](#footnote-ref-15)
15. Section 5.3A.9(2) of the Act. [↑](#footnote-ref-16)
16. Section 6.1.60(1) of the Act. [↑](#footnote-ref-17)
17. Section 5.3A.10A(2) of the Act. [↑](#footnote-ref-18)
18. Section 5.3A.9(4) of the Act. [↑](#footnote-ref-19)
19. Section 5.3A.9A(b) of the Act. [↑](#footnote-ref-20)
20. Section 5.3A.10C of the Act. [↑](#footnote-ref-21)
21. Section 13, Victorian Privacy and Data Protection Act. [↑](#footnote-ref-22)
22. Definition of ‘organisation’ in section 6C of the Commonwealth Privacy Act. [↑](#footnote-ref-23)
23. Section 13, Victorian Privacy and Data Protection Act. [↑](#footnote-ref-24)
24. Personnel of an authorised user includes the officers, employees, agents, contractors and sub-contractors of the authorised user, who are involved in providing or supporting the provision of services connected with the collection, holding, use, management, disclosure or transfer, for or on behalf of the authorised user, of the VSN and related information. [↑](#footnote-ref-25)
25. An information system includes: information technology for the storage and processing of Information, including hardware and software; non-electronic means for storage of information; and procedures for storing, processing, transforming or otherwise dealing with Information, including by use of information technology and non-electronic means. [↑](#footnote-ref-26)
26. Part 6A, *Child Wellbeing and Safety Act 2005*. [↑](#footnote-ref-27)
27. Part 5A, *Family Violence Protection Act 2008*. [↑](#footnote-ref-28)
28. Issued under sections 86 and 87 of the Victorian Privacy and Data Protection Act. [↑](#footnote-ref-29)
29. Part IIIC, *Privacy Act 1988* (Cth). [↑](#footnote-ref-30)
30. See section 38 of the Charter. [↑](#footnote-ref-31)