St Brigid's College
Horsham

Privacy Policy

1. Contents

2. Vision Statement 1
3. Rationale 1
4. Scope 1
5. Policy Statement & Procedures 2
6. Responsibilities 7
7. Legal References 7
8. Related Policies 7
9. Appendices 7
10. Document Review 7

2. Vision Statement

St Brigid's College commits our community to being a child-safe, nurturing and learning environment within the Catholic and Brigidine traditions, where each of us grows to a personal fullness of faith and life.

3. Rationale

This Privacy Policy sets out how the School manages personal information provided to or collected by it.

The School is bound by the Australian Privacy Principles (APPs) contained in the Commonwealth *Privacy Act 1988*. In relation to health records, the School is also bound by the *Health Records Act 2001* (Vic.) and the Health Privacy Principles in that Act.

The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

4. Scope

This policy applies to all members of the College Community

5. Policy Statement & Procedures

What kinds of personal information does the School collect and how does the School collect it?

The School collects and holds personal information, including health and other sensitive information, about:

- students and parents and/or guardians ('Parents') before, during and after the course of a student's enrolment at the School including, but not limited to:
    - name, contact details (including next of kin), date of birth, previous school and religion
    - medical information (e.g. details of disability and/or allergies and details of any assistance the student receives in relation to those disabilities)
    - conduct and complaint records, or other behaviour notes, school attendance and school reports
    - information about referrals to government welfare agencies
    - counselling reports
    - health fund details and Medicare number
    - any court orders
    - volunteering information (including Working With Children Checks)
    - photos and videos at school events.
- job applicants, staff members, volunteers and contractors, including:
    - name, contact details (including next of kin), date of birth and religion
    - information on job application
    - professional development history
    - salary and payment information, including superannuation details
    - medical information (e.g. details of disability and/or allergies and medical certificates)
    - complaint records and investigation reports
    - leave details
    - photos and videos at school events
    - workplace surveillance information
    - work emails and private emails (when using work email address) and internet browsing history
- other people who come into contact with the School, including name and contact details and any other information necessary for the particular contact with the School.

Personal Information you provide: The School will generally collect personal information held about an individual by way of forms filled out by Parents or students, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than Parents and students (such as job applicants and contractors) provide personal information to the School.

Personal Information provided by other people: In some circumstances the School may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school The type of information the School may collect from another school may include:

- academic records and/or achievement levels
- information that may be relevant to assisting the new school meet the needs of the student including any adjustments

Exception in relation to employee records: Under the *Privacy Act*, the Australian Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record where the treatment is directly related to a current or former employment relationship between the School and employee. The School handles staff health records in accordance with the Health Privacy Principles in the *Health Records Act 2001 (Vic.).*

Anonymity*:* The School needs to be able to identify individuals with whom it interacts and to collect identifiable information about them to facilitate the delivery of schooling to its students and its educational and support services, conduct the job application process and fulfill other obligations and processes. However, in some limited circumstances some activities and interactions with the School may be done anonymously where practicable, which may include making an inquiry, complaint or providing feedback.

How will the School use the personal information you provide?

The School will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected by you, or to which you have consented.

Students and Parents: In relation to personal information of students and Parents, the School's primary purpose of collection is to enable the School to provide schooling to students enrolled at the School (including educational and support services for the student), exercise its duty of care and perform necessary associated administrative activities which will enable students to take part in all the activities of the School. This includes satisfying the needs of Parents, the needs of the student and the needs of the School throughout the whole period the student is enrolled at the School.

The purposes for which the School uses personal information of students and Parents include:

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines
- day-to-day administration of the School
- looking after students' educational, social and medical wellbeing
- seeking donations and marketing for the School
- seeking feedback from students and parents on school performance and improvement, including through school improvement surveys
- to satisfy the School's legal obligations and allow the School to discharge its duty of care
- to satisfy the School service providers' legal obligations, including the Catholic Education Commission of Victoria Ltd (CECV) and the Catholic Education Offices.

In some cases where the School requests personal information about a student or Parent, if the information requested is not provided, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

Job applicants and contractors: In relation to personal information of job applicants and contractors, the School's primary purpose of collection is to assess and (if successful) to engage the applicant, or contractor, as the case may be.

The purposes for which the School uses personal information of job applicants and contractors include:

- administering the individual's employment or contract, as the case may be
- for insurance purposes
- seeking donations and marketing for the School
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Volunteers: The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as the School's Alumni association, to enable the School and the volunteers to work together, to confirm their suitability and to manage their visits.

Counsellors: The School contracts with external providers to provide counselling services for some students. The principal may require the Counsellor to inform him or her or other teachers of any issues the principal and the Counsellor believe may be necessary for the School to know for the well-being or development of the student who is counselled or other students at the School.

Parish: The School may disclose limited personal information to the school parish to facilitate religious and sacramental programs, and other activities such as fundraising.

Marketing and fundraising: The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to provide a quality learning environment in which both students and staff thrive. Personal information held by the School may be disclosed to organisations that assist in the School's fundraising, for example, the School's Foundation or alumni organisation [or, on occasions, external fundraising organisations].

Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information and sometimes people's images, may be used for marketing purposes.

Who might the School disclose personal information to and store your information with?

The School may disclose personal information, including sensitive information, held about an individual for **educational, administrative** and **support purposes**. This may include to:

- School service providers which provide educational, support and health services to the School, (either at the School or off campus) including the Catholic Education Commission of Victoria Ltd (CECV), Catholic Education Offices, specialist visiting teachers, volunteers, counsellors, sports coaches and providers of learning and assessment tools
- third party service providers that provide online educational and assessment support services, document and data management services, or applications to schools and school systems including the Integrated Catholic Online Network (ICON) and Google's G Suite, including Gmail and, where necessary, to support the training of selected staff in the use of these services
- other third parties which the school uses to support or enhance the educational or pastoral care services for its students or to facilitate communications with Parents
- another school including to its teachers to facilitate the transfer of a student
- State and Federal government departments and agencies
- health service providers
- recipients of School publications, such as newsletters and magazines
- student's parents or guardians and their emergency contacts
- assessment and educational authorities including the Australian Curriculum, Assessment and Reporting Authority
- anyone you authorise the School to disclose information to
- anyone who we are required or authorised to disclose the information to by law, including child protection laws.

Nationally Consistent Collection of Data (NCCD) on School Students with Disability

The school is required by the Federal *Australian Education Regulation (2013)* and *Australian Education Act 2013* (Cth) (AE Act) to collect and disclose certain information under the *Nationally Consistent Collection of Data* (NCCD) on students with a disability. The school provides the required information at an individual student level

to the Catholic Education Offices and the CECV, as an approved authority. Approved authorities must comply with reporting, record keeping and data quality assurance obligations under the NCCD. Student information provided to the federal government for the purpose of the NCCD does not explicitly identify any student.

Sending and storing information overseas: The School may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual; or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The School may also store personal information [including sensitive information] in the 'cloud'. This means that the information is held on the servers of third party cloud service providers engaged by the School. The servers may be situated in or outside Australia.

The School may from time to time use the services of third party online service providers (including for the delivery of services and third party online applications, or Apps relating to email, instant messaging and education and assessment, such as Google's G Suite, including Gmail) which may be accessible by you. Some personal information [including sensitive information] may be collected and processed or stored by these providers in connection with these services. These online service providers may be located in or outside Australia.

School personnel and the school's service providers, and the CECV and its service providers, may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering the system and services ensuring their proper use.

As not all countries are bound by laws which provide the same level of protection for personal information provided by the APPs, the School makes reasonable efforts to be satisfied about the security of any personal information collected, processed and stored outside Australia, including that of cloud and third party service providers.

The countries in which the servers of cloud service providers and other third party service providers are located may include:

- United States of America , India, Canada, United Kingdom, France, Germany, Sweden
- Other countries from time to time

Where personal and sensitive information is retained by a cloud service provider on behalf of CECV to facilitate Human Resources and staff administrative support, this information may be stored on servers located in or outside Australia.

How does the School treat sensitive information?

In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Management and security of personal information

The School's staff are required to respect the confidentiality of students' and Parents' personal information and the privacy of individuals.

The School has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records. This includes responding to any incidents which may affect the security of the personal information it holds. If we assess that anyone whose information is affected by such a breach is likely to suffer serious harm as a result, we will notify them and the Office of the Australian Information Commissioner of the breach. It is recommended that parents and the school community adopt secure practices to protect themselves. You should ensure that all passwords you use are strong and regularly updated and that your log in details are kept secure. Do not share your personal information with anyone without first verifying their identity and organisation. If you believe any of your personal information has been compromised, please let the School know immediately.

Access and correction of personal information

Under the Privacy Act and the Health Records Act, an individual has the right to seek and obtain access to any personal information and health records respectively which the School holds about them and to advise the School of any perceived inaccuracy. Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves.

There are some exceptions to the access rights set out in the applicable legislation.

To make a request to access or to update any personal information the School holds about you or your child, please contact the School Principal or School Admin Office by telephone or in writing. The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

There may be circumstances where the reason for refusal is not provided, if doing so may breach the privacy of another person.

Consent and rights of access to the personal information of students

The School respects every Parent's right to make decisions concerning their child's education.

Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. The School will treat consent given by Parents as consent given on behalf of the student, and notice to Parents will act as notice given to the student.

Parents may seek access to personal information held by the School about them or their child by contacting the School Principal or School Administration Office by telephone or in writing. However, there may be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student.

The School may, at its discretion, on the request of a student grant that student access to information held by the School about them, or allow a student to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

6. Responsibilities

Enquiries and complaints and contact details

If you would like further information about the way the School manages the personal information it holds about you, or wish to complain that you believe that the School has breached its privacy obligations, please contact the School Principal by writing or telephone at PO Box 542, Horsham VIC 3400 or (03) 5382 3545. The School will investigate your complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

If you are not satisfied with the School's decision you may make a complaint to the Office of the Australian Information Commissioner (OAIC) whose contact details are:
GPO Box 5218, Sydney, NSW 2001
Telephone: 1300 363 992
www.oaic.gov.au

7. Legal References

Federal and relevant State laws bind the School and its employees. A breach of this policy may result in the School and/or its employees breaching any one of the following pieces of legislation:

Commonwealth

Australian Privacy Principles (APPs) contained in the Commonwealth *Privacy Act 1988*.
Health Records Act 2001 (Vic.) and the Health Privacy Principles in that Act.

Also;
Disability Discrimination Act 1992 (Cth);
Education and Training Reform Act 2006 (Cth)
Victoria
Child Safe Standards (Ministerial Order 870)
Note: This is not an exhaustive list of the relevant legislation.

8. Related Policies

Child Safety Policy
Child Safety – Mandatory reporting & Other Obligations Policy

9. Appendices

- Appendix I - Privacy Policy – Information Collection Notice (3 Pages)
- Appendix II – Data Breach Response Plan (17 Pages)

10. Document Review

Prepared: Mar 2014	**Date**	**Comment**
Updated:	May 2018	Inclusion of new NCCD and NDB Scheme requirements
Updated:	Apr 2019	Include reference to 'school improvement surveys'
Updated:	Mar 2020	Additional clauses
Due for Review:	**May 2022**	

Information Collection Notice

1. The School collects personal information, including sensitive information about students and parents or guardians and family members before and during the course of a student's enrolment at the School. This may be in writing or in the course of conversations and may be direct from the individual or from another source. The primary purpose of collecting this information is to enable the School, Catholic Education Offices and the Catholic Education Commission of Victoria Ltd (CECV) to meet its educational, administrative and duty of care responsibilities to the student to enable them to take part in all the activities of the School.

2. Some of the information the School collects is to satisfy the School's legal obligations, particularly to enable the School to discharge its duty of care.

3. Laws governing or relating to the operation of a school require certain information to be collected and disclosed. These include relevant Education Acts and Public Health and Child Protection laws.

4. Health information about students (which includes information about any disability) is sensitive information within the terms of the Australian Privacy Principles (APPs) under the *Privacy Act 1988*. The School may request medical reports about students from time to time and may otherwise collect sensitive information about students and their families.

5. If any personal information requested by the School is not provided, this may affect the School's ability to enrol a student, respond to enquiries, provide the student with educational and support services or allow a person to visit the School.

6. The School may disclose personal and sensitive information for **administrative, educational** and **support purposes** (or may permit the information to be directly collected by third parties). This may include to:

- School service providers such as the CECV, Catholic Education Offices, school governing bodies and other dioceses
- third party service providers that provide online educational and assessment support services or applications (apps) such as Skoolbag, or services in relation to school improvement surveys, which may include email and instant messaging
- School systems, including SIMON, the Integrated Catholic Online Network (ICON), Microsoft 365 and Google's 'G Suite' including Gmail. Limited personal information may be collected and processed or stored by these providers in connection with these services
- CECV to undertake financial modelling for students with a disability, including ongoing evaluation of funding adequacy for individual students
- CECV to support the training of selected staff in the use of schools' systems, such as ICON
- another school to facilitate the transfer of a student
- Federal and State government departments and agencies
- health service providers, and people providing educational support and health services to the School, including specialist visiting teachers, sports coaches, volunteers, counsellors and providers of learning and assessment tools
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority
- people providing administrative and financial services to the School
- anyone you authorise the School to disclose information to; and

- anyone to whom the School is required or authorised to disclose the information to by law, including under child protection laws.

7. The school is required by the Federal *Australian Education Regulation (2013) and Australian Education Act 2013* (Cth) (AE Act) to collect and disclose certain information under the *Nationally Consistent Collection of Data* (NCCD) on students with a disability. The school provides the required information at an individual student level to the Catholic Education Offices and the CECV, as an approved authority. Approved authorities must comply with reporting, record keeping and data quality assurance obligations under the NCCD. Student information provided to the federal government for the purpose of the NCCD does not explicitly identify any student.

8. Personal information collected from students is regularly disclosed to their parents or guardians.

9. The School may also use cloud computing service providers to store personal information (which may include sensitive information) on their servers in the 'cloud'. These servers may be located in or outside Australia. This may mean that personal information may be stored or processed outside Australia.

10. As not all countries are bound by laws which provide the same level of protection for personal information as the APPs, the School makes reasonable efforts to be satisfied about the protection of any personal information that may be collected, processed and stored outside Australia in connection with any cloud and third party services.

11. When the School uses Microsoft 365 and/or Google's G-Suite including Gmail, some personal information (usually limited to name and email address) of students, parents or guardians may be transferred, stored and processed by Google in the United States, or in any other country through which Google provides these services or where it processes and stores information. This personal information will be stored and processed by Google in accordance with Google's terms and conditions stated in the G-Suite for Education Agreement which the school entered into with Google.

12. The School's Privacy Policy contains further information about its use of cloud and other third-party service providers and any of their overseas locations.

13. Where personal, including sensitive information is held by a cloud computing service provider on behalf of CECV for educational and administrative purposes, it may be stored on servers located within or outside Australia. This includes the ICON system.

14. School personnel and the school's service providers, and the CECV and its service providers, may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering the ICON system and ensuring its proper use.

15. The School may disclose limited personal information to the school parish to facilitate religious and sacramental programs, and other activities such as fundraising.

16. The School's Privacy Policy is accessible via the school website, newsletter, handbook, or from the School office. The policy sets out how parents, guardians or students may seek access to, and correction of their personal information which the School has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others, or may result in a breach of the School's duty of care to the student, or where students have provided information in confidence. Any refusal will be notified in writing with reasons if appropriate.

17. The School's Privacy Policy also sets out how parents, guardians, students and their family can make a complaint if they believe the School has interfered with their privacy, and how the complaint will be handled.

18. The School may engage in fundraising activities. Information received from you may be used to make an appeal to you. It may also be disclosed to organisations that assist in the School's

fundraising activities solely for that purpose. We will not disclose your personal information to third parties for their own marketing purposes without your consent.

19. On occasions information such as academic and sporting achievements, student activities and similar news is published in School newsletters and magazines, on our intranet and on our website. This may include photographs and videos of student activities such as sporting events, school camps and school excursions. The School will obtain permissions from the student's parent or guardian (and from the student if appropriate) prior to publication to enable the school to include such photographs or videos [or other identifying material] in our promotional material or otherwise make this material available to the public such as on the internet. The school may obtain permissions annually, or as part of the enrolment process. Permissions obtained at enrolment may apply for the duration of the student's enrolment at the school unless the school is notified otherwise. Annually, the school will remind parents and guardians to notify the school if they wish to vary the permissions previously provided. We may include student's and parents' or guardians' contact details in a class list and School directory.

20. If you provide the School with the personal information of others, such as other family members, doctors or emergency contacts, we encourage you to inform them you are disclosing that information to the School and why, that they can request access to and correction of that information if they wish and to also refer them to the School's Privacy Policy for further details about such requests and how the School otherwise handles personal information it collects and complaints it receives.

Data Breach Response Plan

This data breach response plan (response plan) sets out procedures in the event that St Brigid's College experiences a data breach (or suspects that a data breach has occurred).

Definition

Data Breach

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

Notifiable Data Breach

Where a data breach has occurred that is likely to result in serious harm to any of the individual to whom the information relates, it is considered *'eligible'* and must be reported to the Office of the Australian Information Commissioner (OAIC)

Implementation

This response plan is intended to enable the St Brigid's College to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It clarifies the roles and responsibilities of staff, and the processes to assist the school to respond to a data breach (refer to Appendix A: Flow Chart: Data Breach Response Plan).

Some data breaches may be comparatively minor, and able to be dealt with easily without reporting to the OAIC. For example:

> *A staff member, as a result of human error, sends an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that the issue is reported to the principal but does not require any further response.*

This should be documented including:

- Description of breach or suspected breach
- Action taken by the principal to address the breach or suspected breach
- The outcome of the action
- The principal's view that no further action is required

The principal will use their discretion in determining whether a data breach or suspected data breach requires an escalation of the data breach process. In making that determination, principal will consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in school processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then it may be appropriate for the principal to notify the OAIC (refer to Risk Assessment Process).

OAIC Advice Data Breach: What must be included will assist the principal in notifying the OAIC. https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-notification-guide-august-2014.pdf

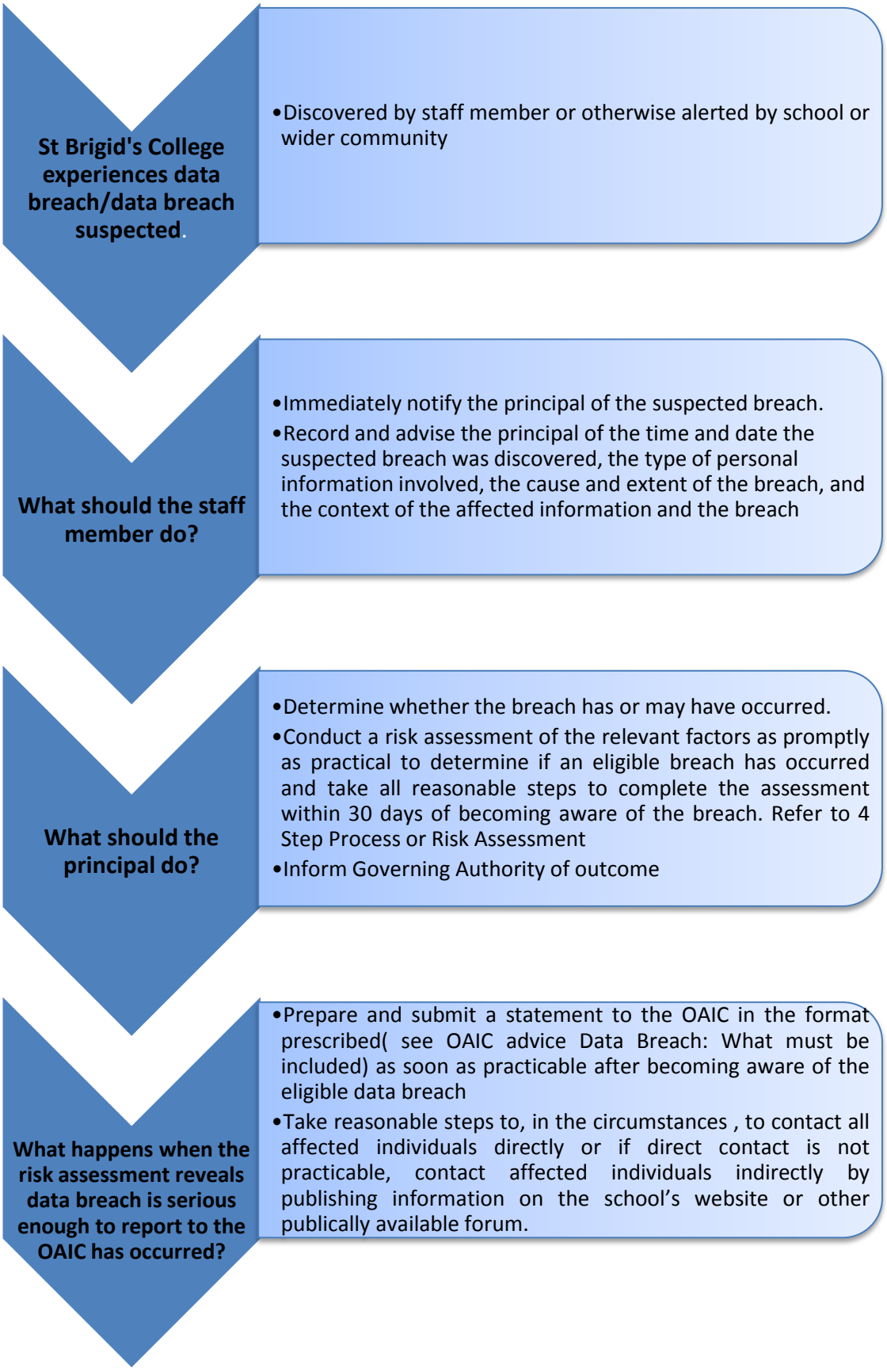
Record Management

Documents on breaches will be saved in a central file on school administration system.

Refer to:

- Appendix A: Flow Chart: Data Breach Response Plan
- Appendix B: Risk Assessment Process
- Appendix C: Data Breach Prevention Checklist (CECV)
- Appendix D: Individual Notification Record (CECV)
- Appendix E: Example of an Email to Parents/Carers (CECV)
- Appendix F: Data Breach Notification for Other Entities (CECV)
- Appendix G: Notification Procedures Checklist (CECV)
- Appendix H: Contain the Breach and Preliminary Assessment (CECV)
- Appendix I: Evaluate Risks (CECV)

Appendix A:
Flow Chart: Data Breach Response Plan



Appendix B: Risk Assessment Process

Step 1: Contain the breach and do a preliminary assessment

- Convene a meeting with relevant staff and/or Leadership Team
- Ensure that all evidence of breach is preserved so that an assessment of the breach can be made

STEP 2: Evaluate the Risks Associated with the Breach

- Conduct an initial investigation, and collect information about the breach promptly including;
    - The date, time, duration and location of the breach
    - The type of personal information involved in the breach
    - How the breach was discovered and by whom
    - The cause and extent of the breach
    - A list of affected individuals, or possible affected individuals
    - The risk of serious harm to the affected individuals
    - The risk of other harms

- Determine whether the content of the information is important
- Establish the cause and effect of the breach
- Assess priorities and risks based on what is known
- Keep appropriate records of the suspected breach and actions of the response team, including the stapes taken to rectify the situation and the decisions made

STEP 3: Notification

- Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage
- Determine whether to notify affected individuals is there a real risk of serious harm to the affected individuals? In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where the school is contractually required or required under the terms of an MOU or similar obligation to notify specific parties

STEP 4: Prevent Future Breaches

- Fully investigate the cause of the breach
- Report to Governing Authority on outcomes and recommendations:
    - Update security and response plan if necessary.
    - Make appropriate changes to policies and procedures if necessary
    - Revise staff training practices if necessary
    - Consider the option of an audit to ensure necessary outcomes are affected

Appendix C: Data Breach Prevention Checklist (CECV)

Item to be checked	*Setup correct*	*Comments*
PHYSICAL CHECKS		
Servers and computers, and storage devices storing data which have the potential to harm individuals or the school are stored in a locked and alarmed area after hours.		
Access to these areas are restricted to authorized personnel by means of separate key types and security codes.		
All areas are checked that they are securely shut at the end of each day.		
Alarmed areas are checked when alarms are activated.		
Stolen computers to be reported to police.		
Paper records are shredded or disposed of by placing in a locked bin and properly disposed of by a professional company hired for the purpose.		
Security contractors check the campus daily.		
COMPUTER SECURITY		
All computers require password login.		
Staff passwords are required to be changed regularly according to a set security procedure.		
Access to various data is governed by login credentials.		
Bulk transfer of data on removable media is to be avoided but may be approved by management and removed from media after transfer		
Bulk download of data is to be avoided but may be approved by management if required. Data is deleted from computers after specific use.		
Bulk communication (email, SMS) do not allow users to see others' data (Use of Bcc in emails)		
Erasing of all data on laptops before they are permanently removed from the school (staff and students leaving; laptops donated to others)		
NETWORK SECURITY		
Administration access by restricted personnel.		
Firewall rules set to prevent unauthorized access.		
Student and staff networks are separated.		
Intranet access is restricted by network login credentials or parental login credentials.		
COMMUNICATIONS SECURITY		
Student email is web-based and filtered for unauthorized access and malware.		
Staff email is server-based and filtered for unauthorized access and malware.		

PERSONNEL SECURITY		
Visitors need to sign a register when arriving and leaving the campus.		
Locks to servers or areas containing classified information are different to the general locks to areas accessible for general staff.		
Keys are allocated to staff according to security clearance level.		
Contractors are supervised on campus.		

POLICIES and PROCEDURES		
Privacy Policy available on school website for anyone to review		
Staff, students, parents and affected others are made aware of the school's privacy policy.		
Procedures available to govern the collection, input, access, retention and disposal of data		
Approval of all service delivery partners' privacy policies		
TRAINING		
Staff training on correct procedures involving the collection, input, access, retention and disposal of data		

Appendix D: Individual Notification Record (CECV)

Date of breach: **Time of breach**:
Date and time breach was reported:
Data Breach Description:
Assessed level of risk:
Individual directly affected:
There may be circumstances where parents, carers or authorised representatives should be notified as well as, or instead of, the individual.

Individual Notification

Person notified	Person sending notification	Contact details of person notified	Notification Date	Acknowledgement date

Notification Details:

A copy of email or written description sent to the individual should be placed below and should include the following headings:

- **Incident Description** and **Type of personal information involved**
- **Response to the breach**
- **Assistance offered to affected individuals**
- **School contact details —**
- **How individuals can lodge a complaint with the school —**

Appendix E: Example of an email to Parents/Carers (CECV)

Dear Mr. and Mrs. Smith
We are writing to inform you of an incident that has the possibility of exposing your contact information to unauthorised people or organisations.
On June 8, 2107, a CEM staff members USB memory stick with a file containing your names, your home address, email addresses and phone numbers (home and mobile) was reported missing. While we are attempting to locate the USB stick, we believe it would be prudent to consider any actions you need to take to mitigate and possible harm.
In particular, please take note of any unsolicited calls or emails. Should such events occur, please consider changing your details and please inform the school of such occurrences and inform us of your new contact details.
We sincerely apologise for the inconvenience or harm this may cause. We are reviewing our procedures regarding the storage of sensitive information on portable media such as USB memory sticks and will implement any procedural changes required in an attempt to avoid such events in future.
Please don't hesitate to contact me if you wish to discuss the matter further.

Sincerely,

Principal
St Brigid's College

Form:

This form should be used when preparing to inform other entities that may be impacted by the data breach.

Complete each section

1. **A description of the breach**
2. **The type of personal information involved**
3. **How many people were or may have been affected**
4. **When the breach occurred**
5. **When and how the school became aware of the breach**
6. **The cause of the breach**
7. **Whether the breach was inadvertent or intentional**
8. **Whether the breach appears to stem from a systemic issue or an isolated trigger**
9. **Whether the breach has been contained**
10. **What action has been taken or is being taken to mitigate the effect of the breach and/or prevent further breaches**
11. **Any other entities involved**
12. **Whether the school has experienced a similar breach in the past**
13. **Any measures that were already in place to prevent the breach**
14. **Whether a data breach response plan was in place, and if it has been activated**
15. **The name and contact details of an appropriate person within your organisation**
16. **Any other relevant factors.**

Appendix G: Notification Procedures Checklist (CECV)

Date of breach: **Time of breach**:
Date and time breach was reported:
Data Breach Description:
Assess level of risk: *(Circle)*

- High (potential for immediate harm):
  - Take steps to notify individuals –
  - Assess need to notify others – See ***Obligations to notify others*** below
- Medium (potential for inconvenience and disruption):
  - Assess need to notify
- Low (mainly related to temporary information which will change over time):
  - Assess need to notify

Assess obligations to notify others:
Check obligations in the list below.
If required, complete the form: Data Breach Notification for Other Entities

- *Third party 'cloud' data storage provider*
- ***OAIC*** *– The following factors should be considered in deciding whether to report a breach to the OAIC:*
  - *any applicable legislation that may require notification*
  - *the type of the personal information involved and whether there is a* ***real risk of serious harm*** *arising from the breach, including non-monetary losses*
  - *whether a large number of people were affected by the breach*
  - *whether the information was fully recovered without further disclosure*
  - *whether the affected individuals have been notified, and*
  - *if there is a reasonable expectation that the OAIC may receive complaints or inquiries about the breach*
- ***Police —*** *If theft or other crime is suspected. The Australian Federal Police should also be contacted if the breach may constitute a threat to national security.*
- **Insurers or others —** If required by contractual obligations
- **Credit card companies, financial institutions or credit reporting agencies –** If their assistance is necessary for contacting individuals or assisting with mitigating harm.
- ***Professional or other regulatory bodies —*** *If professional or regulatory standards require notification of these bodies*
- ***Other internal or external parties not already notified —*** *Consider the potential impact that the breach and notification to individuals may have on third parties, and take action accordingly. For example, school accounts department might be affected if individuals cancel their credit cards, or if financial institutions issue new cards.*
- *Consider:*
  - *third party contractors or other parties who may be affected*
  - *internal business units not previously advised of the breach, (for example, communications and media relations, senior management), or*
  - *union or other employee representatives*

- ***Agencies that have a direct relationship with the information lost/stolen —*** *The school should consider whether an incident compromises Australian Government agency identifiers such as TFNs or Medicare numbers. Notifying agencies such as the Australian Taxation Office for TFNs or Medicare Australia for Medicare card numbers may enable those agencies to provide appropriate information and assistance to affected individuals, and to take steps to protect the integrity of identifiers that may be used in identity theft or other fraud.*

Overall Assessment:

- Assessed to not require notification of other entities
    - Not broad enough in numbers of parents/carers affected
    - Not enough to cause serious harm – complete identity theft
    - Not determined if theft occurred

Checklist

Date of breach: **Time of breach**:
Date and time breach was reported:
Data Breach Description:

Action	Person/s Responsible	Comment
CONTAIN THE BREACH		
Stop the unauthorised practice		
Recover the records		
If possible or if it would not compromise evidence, shut down the system that was breached		
If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges		
Address weaknesses in physical or electronic security		
PRELIMINARY ASSESSMENT		
Appoint someone to lead the initial assessment		
Is there is a need to assemble a team		
What personal information does the breach involve?		
What was the cause of the breach?		
What is the extent of the breach?		
What are the harms (to affected individuals) that could potentially be caused by the breach?		
How can the breach be contained?		

EARLY NOTIFICATION		
Who needs to be made aware of the breach (internally, and potentially externally)?		
List affected individuals		
Escalate to management as appropriate – person for privacy compliance		
Do police need to be informed?		
Is serious harm to individuals possible?		
Is high level media attention likely?		
Complete "Notification Record" (Step 3)		
OTHER MATTERS		
If laws have been broken, consult before going public with details		
Be careful not to destroy evidence		
Keep records of the suspected breach and the steps taken to rectify the situation and the decisions that are made.		

Checklist

Complete the following sections:

1. Description of the breach and the extent of the breach

Date of breach: **Time of breach**:
Date and time breach was reported:
Data Breach Description:

What was the source of the breach?

Who discovered / reported the initial breach?

Who was this reported to?

What parties have gained unauthorised access to affected information?

What was the context of the breach?

What was the extent of the unauthorised access?

Any other related breaches which could have a cumulative affect?

Is there evidence of theft?

Level of encryption/ anonymisation of information –

Has the personal information been recovered?

Is this a systemic problem or an isolated incident?

2. Type of personal information involved in the breach

Personal identification:
Financial:
Medical:
Personnel records:
Assessment records:
Combination of information types:
Other:

3. Who is affected by the breach?

Employees:
Contractors:
General public:
Students:
Parents:
Service providers:
Other agencies or organisations:

4. Assessment of level of harm – select and give a reason

High (potential for immediate harm): parent personal details; student records editable
Medium (potential for inconvenience and disruption):
Low (mainly related to temporary information which will change over time):
Which of the following are possible as a result of the breach?
A) Harm to the person

- *identity theft*
- *financial loss*
- *threat to physical safety*
- *threat to emotional wellbeing*
- *loss of business or employment opportunities*
- *humiliation, damage to reputation or relationships, or*
- *workplace or social bullying or marginalization*

B) Harm to CEM/CECV Offices and Schools

- *the loss of public trust*
- *reputational damage*
- *loss of assets (e.g., stolen computers or storage devices)*
- *financial exposure (e.g., if bank account details are compromised)*
- *regulatory penalties (e.g., for breaches of the Privacy Act)*
- *extortion*
- *legal liability*
- *breach of secrecy provisions in applicable legislation*