Privacy Policy and Guideline

CANBERRA CHRISTIAN SCHOOL

NURTURE | LEARNING | CHARACTER

TABLE OF CONTENTS

---

1. Rationale

Canberra Christian School (CCS) recognises and affirms the view that all people possess innate dignity, worth and a right to privacy. From this stem the principles of respect, kindness and transparency.

CCS seeks to protect and maintain dignity through sensitive, ethical and culturally aware use of personal information. In doing so, the School will comply with the Australian Privacy Principles contained in the Commonwealth Privacy Act.

2. Definitions

Term	Definition
Director	Executive Director or Associate Executive Director or delegate
Responsible person for a school	1. Each director on the Schools' Company board 2. The principal of the school
Schools' Company	One of: Seventh-day Adventist Schools (Greater Sydney) Ltd Seventh-day Adventist Schools (NNSW) Ltd Seventh-day Adventist Schools (SNSW) Ltd

3. Policy Statement

This policy applies to all employees, students, volunteers and contractors involved in the collection, use, holding or disclosure of personal information on behalf of the School.

1. **Personal Information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not. Examples include an individual's name, address, contact number and email address.
2. **Sensitive Information** is a special category of personal information. Canberra Christian School may collect personal information which is "sensitive information".

Such information includes:

- criminal records;
- health information;
- genetic information about an individual that is not otherwise health information
- biometric information;
- political, philosophical, religious opinions or beliefs;
- membership of professional or trade associations
- information concerning sexual orientation and practices; and
- information about racial and ethnic origin.

3. **Health Information** includes information or an opinion about:

- the health or disability of an individual; and
- a health service to be provided to the individual.

4. **Employee Record** is defined broadly to be a record of personal information relating to the employment of an employee. Examples of this type of information include the terms and conditions of employment, personal contact details, performance and conduct, disciplining, salary, termination and trade union

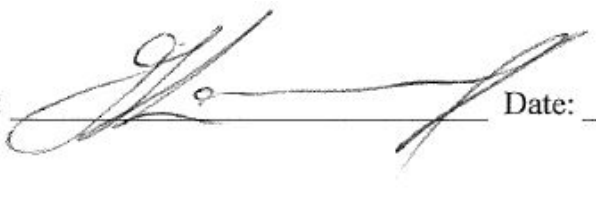
4. Implementation

The School is bound by the Australian Privacy Principles contained in the Privacy Act 1988 (Cth) (Privacy Act) and the School is also bound by the Health Records and Information Privacy Act 2002 (NSW) (Health Records Act), or equivalent legislation in other States/Territories (e.g. Victorian Health Records Act 2001) in relation to health records held by the School.

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

5. Date of next policy review

- July 2020

Council Chair Signature:  Date: 1/5/19

6. Privacy Policy Guidelines

6.1. What kinds of personal information does a school collect and how does a school collect it?

The type of information schools collect and hold includes (but is not limited to) personal information, including health and other sensitive information, about:

1. pupils and parents and/or guardians (*Parents*) before, during and after the course of a pupil's enrolment at the school;
2. job applicants, staff members, volunteers and contractors; and
3. other people who come into contact with the school.

6.2. Personal Information you provide:

A school will generally collect personal information held about an individual by way of forms filled out by *Parents* or pupils, face-to-face meetings and interviews, emails, telephone calls and the capture of still and moving images. On occasions people other than *Parents* and pupils provide personal information.

6.3. Personal Information provided by other people:

In some circumstances a 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.

6.4. Exception in relation to employee records:

The Privacy Act and the Australian Privacy Principles do not apply to an employee's 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.

6.5. How will a school use the personal information you provide?

A 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, or to which you have consented.

6.6. Pupils and parents

In relation to personal information of pupils and *Parents*, a school's *primary purpose of collection* is to enable the school to provide schooling for the pupil. This includes satisfying the needs of *Parents*, the needs of the pupil, the needs of school and *the Schools' Company* throughout the whole period the pupil is enrolled at the school. The purposes for which the school and *the Schools' Company* uses personal information of pupils and *Parents* include:

1. to keep *Parents* informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
2. day-to-day administration;
3. looking after pupils' educational, social, spiritual and medical wellbeing;
4. documenting school events and educational experiences through the collection of still and moving images presented or made available to members of the school community in printed or electronic form;
5. seeking donations and marketing for the school; and
6. to satisfy the school's and *the Schools' Company's* legal obligations and allow the school to discharge its duty of care including the appropriate handling of Child Protection matters. In some cases where a school requests personal information about a pupil or *Parent*, if the information requested is not obtained, the school may not be able to enrol or continue the enrolment of the pupil or permit the pupil to take part in a particular activity.

6.7. Job applicants, staff members and contractors

In relation to personal information of job applicants, staff members and contractors, a school's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be. The purposes for which a school uses personal information of job applicants, staff members and contractors include:

1. in administering the individual's employment or contract, as the case may be;
2. for insurance purposes;
3. seeking funds and marketing for the school; and

4. to satisfy the school's and *the Schools' Company's* legal obligations, for example, in relation to child protection legislation.

6.8. Volunteers

A school also obtains personal information about volunteers who assist the school in its functions or conduct associated activities, such as the school's Home and School Association, to enable the school and the volunteers to work together.

6.9. Marketing and fundraising

Schools treat marketing and seeking donations for the future growth and development of the school as an important part of ensuring that the school continues to be a quality learning environment in which both pupils and staff thrive. Personal information held by a school may be disclosed to an organisation that assists 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, may be used for marketing purposes.

6.10. Exception in relation to related schools

The Privacy Act allows each school, being legally related to each of the other schools operated by *the Schools' Company* to share personal (but not sensitive) information. Other Schools' Company, schools may then only use this personal information for the purpose for which it was originally collected by the original school. This allows schools to transfer information between them, for example, when a pupil transfers between Schools' Company schools.

7. Who might a school disclose personal information to and store your information with?

A school may disclose personal information, including sensitive information, held about an individual to:

1. child protection agencies including AdSAFE, the church's child protection service;
2. another school;
3. government departments;
4. the school's local church??;
5. medical practitioners;
6. people providing services to the school, including specialist visiting teachers, counsellors and sports coaches;
7. recipients of school publications, such as newsletters and magazines;
8. *Parents*;
9. anyone you authorise the school to disclose information to; and
10. anyone to whom we are required to disclose the information by law.

7.1. Sending and storing information overseas:

A school may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, a school will not send personal information about an individual outside Australia without:

1. obtaining the consent of the individual (in some cases this consent will be implied); or
2. otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.
3. The school may also store personal information in the 'cloud' which may mean that it resides on servers which are situated outside Australia.

8. How does a school treat sensitive information?

In referring to 'sensitive information', a 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.

9. Management and security of personal information

The staff from the schools and *the Schools' Company* are required to respect the confidentiality of pupils' and *Parents'* personal information and the privacy of individuals. Each 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.

10. Access and correction of personal information

Under the Commonwealth Privacy Act and the Health Records and Information Privacy Act 2002 NSW an individual has the right to obtain access to any personal information which the school or *the Schools' Company* holds about them and to advise these organisations of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Pupils will generally be able to access and update their personal information through their Parents, but older pupils may seek access and correction themselves. There are some exceptions to these rights set out in the applicable legislation. To make a request to access or update any personal information the school or *the Schools' Company* holds about you or your child, please contact the School's Principal 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.

11. Consent and rights of access to the personal information of pupils

The Schools' Company respects every *Parent's* right to make decisions concerning their child's education.

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

As mentioned above, parents may seek access to personal information held by a school or *the Schools' Company* about them or their child by contacting the School's Principal. However, there will 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 pupil.

A school may, at its discretion, on the request of a pupil grant that pupil access to information held by the school about them, or allow a pupil 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 pupil and/or the pupil's personal circumstances so warranted.

12. Responding to Data Breaches

12.1. Introduction

7.1.1 A data breach concerns the security of personal information and involves the actual unauthorised access or disclosure of personal information, or the loss of personal information where the loss is likely to result in unauthorised access or disclosure (**Data Breach**).

7.1.2 Data Breaches are not limited to the malicious acts of third parties, such as theft or 'hacking', but may also arise from human error, a systems failure, or a failure to follow information handling or data security policies resulting in accidental loss, access or disclosure. Data Breaches are different from an interference with privacy that involves a breach of another privacy principle such as a use or disclosure of personal information which is not permitted under APP6 (see ' Section 9 – Use or disclosure of personal information). The following are examples of when a Data Breach may occur:

1. loss of smartphone or other School device or equipment containing personal information;
2. cyber attacks on the School's system, resulting in unknown third parties accessing or stealing personal information;
3. accidental transmission of personal information such as student's reports to unintended recipients via e-mail;
4. loss or theft of hard copy documents; and
5. misuse of personal information of students or parents by School personnel.

7.1.3 From 22 February 2018, all agencies and organisations with existing personal information security obligations under the Privacy Act, including Schools, will be required to report certain data breaches under the notifiable data breaches scheme (**NDB Scheme**). The NDB Scheme was inserted into the Privacy Act by the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth). It sets out obligations to notify affected individuals and the Information Commissioner about data breaches which fall within the definition of an eligible data breach' (**EDB**).

7.1.4 A Data Breach is an EDB if it is likely to result in serious harm to an individual or individuals whose information is involved in the Data Breach. Not all Data Breaches will be EDBs. For example, if a School acts quickly to remediate a Data Breach, and as a result of this action the Data Breach is not likely to result in serious harm, there is no obligation to notify any individuals or the Information Commissioner. However, in some cases, a School may decide to voluntarily notify individuals and/or the Information Commissioner. There are also limited exceptions to notifying affected individuals and the Information Commissioner of an EDB in certain circumstances.

7.1.5 This Section provides guidance for Schools regarding:

1. containing a Data Breach;
2. assessing whether a Data Breach is an EDB and taking remedial action to reduce the likelihood of harm to individuals affected by the Data Breach;
3. notifying the Information Commissioner of an EDB and notifying individuals affected by an EDB, and potential exceptions to notification; and
4. reviewing the Data Breach/EDB.

7.1.6 Additional useful resources:

a. the OAIC's *NDB Scheme: Resources for agencies and organisations* available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme (**OAIC Resources**);
b. the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) (**Amending Act**); and
c. the explanatory memorandum for the Privacy Amendment (Notifiable Data Breaches) Bill (**Explanatory Memorandum**).

12.2. Containing the Data Breach

7.2.1 Once a School suspects a Data Breach may have occurred, immediate steps should be taken to identify the Data Breach and if a Data Breach has occurred, to contain and limit it.This may involve stopping the unauthorised disclosure, shutting down the system that was breached, retrieving personal information, or changing computer access privileges or addressing security weaknesses.

12.3. Assessing whether the Data Breach is an EDB

7.3.1 Schools also need to determine whether the Data Breach is an EDB. This involves assessing whether:

a. there has been unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information in circumstances where the loss is likely to result in unauthorised access or disclosure; and
b. if so, the Data Breach is likely to result in serious harm to any of the individuals whose personal information was involved; and
c. remedial action is possible.

7.3.2 Is serious harm likely?

a. Determining whether serious harm is likely is a threshold test and involves considering whether a reasonable person in the School's position would conclude that the Data Breach would be likely (more probable than not) to result in serious harm to any of the individuals to whom the information relates.
b. This reasonable person test is aimed at ensuring only EDBs are reported to the Information Commissioner – not every Data Breach. EDBs will be Data Breaches:
    i. that a reasonable person in the School's position (rather than the individual to whom the information relates or any other person) would conclude,
    ii. based on all of the information either immediately available to them, or available following reasonable inquiries or an assessment of the data breach,
    iii. that the unauthorised access to or disclosure of the particular personal information or the particular individual, is likely to result in serious harm to them.
c. This test is designed to support the objective of the Privacy Act to promote the protection of the privacy of individuals while balancing the interests of entities carrying out their legitimate functions or activities. It also helps avoid unnecessary administrative burdens (both on entities such as Schools, and on the OAIC receiving notification), and 'notification fatigue' on the part of individuals.

7.3.3 What is serious harm?

a. Serious harm is not defined in the Privacy Act, however in the context of a Data Breach, the OAIC Resources note that serious harm may include serious physical, psychological, emotional, financial or reputational harm. The Privacy Act also sets out a non-exhaustive list of 'relevant matters' that may assist Schools in assessing the likelihood of serious harm. These include:
    i. the kind or kinds of personal information involved;
    ii. the sensitivity of that information;
    iii. whether the information is protected by one or more security measures and the likelihood any such security measures would be overcome, including the use of an encryption key to circumvent the encryption technology or methodology;
    iv. the person, or the kinds of persons, who have obtained, or who could obtain, the information;
    v. the likelihood that the person who has obtained the information, or has or could obtain, the information or knowledge required to circumvent the security technology or methodology;
    vi. the nature of the harm; and
    vii. any other relevant matters.
b. Each factor is explored in more detail in Annexure 8.

7.3.4 Can serious harm be prevented with remedial action?

a. As part of assessing the likelihood of serious harm, Schools should take steps to consider whether remedial action to reduce any potential harm to individuals is possible (to prevent serious harm). The NDB Scheme provides that if entities take remedial action to prevent serious harm resulting from the Data Breach, then it will not be a Data Breach that must be notified. The School will need to assess whether the effect of the action it takes would mean that the Data Breach would not be likely to result in serious harm to any of the individuals to whom the affected information relates in relation to any remedial action. This may include action taken in relation to:
    i. the access or disclosure that has occurred *before* the access or disclosure results in serious harm to any of the individuals to whom the information relates; or
    ii. the loss of information *before* there is unauthorised access to or disclosure of the information so that there is no unauthorised access or unauthorised disclosure; or
    iii. the loss of information *after* there is an unauthorised access to or disclosure but *before* the access or disclosure results in serious harm to any of the individuals to whom the information relates.

7.3.5 Timing of the assessment

a. If Schools suspect an EDB may have occurred, they should take reasonable steps to conduct this assessment expeditiously, and where possible, within 30 days after the suspicion arises that a Data Breach has occurred. A sample data breach response plan is set out in Annexure 8.

7.3.6 What if multiple organisation are involved in the EDB or suspected EDB?

a. If a School or other organisation (eg a cloud service provider or other third party supplier) are together involved in a Data Breach affecting personal information of individuals the School handles, and either the School or other organisation has made an assessment about a suspected Data breach to determine whether there has been an EDB, the School or other organisation involved in the Data Breach is not required to undertake the same assessment and may rely on the assessment already made. Despite this, in some cases Schools may also want to undertake their own assessment or may have information that would help determine whether serious harm is likely to any individual.

12.4. Notifying individuals and the Information Commissioner

7.4.1 Once a School is aware that there are reasonable grounds to believe there has been an EDB, the School must, as soon as practicable:

a. make a decision about which individuals to notify;
b. prepare a statement for the Information Commissioner in accordance with the OAIC *Notifiable Data Breach statement – Form* – this can be emailed or lodged online via the OAIC website; and
c. notify individuals of this statement as soon as practicable after notifying the Information Commissioner.

7.4.2 The School will still need to be continuing to take what steps it can to contain the Data Breach and minimise the likely harm as well as deciding what steps it would recommend the individuals can take to protect themselves as it will need to explain this in the statement it must give to the Information Commissioner and individuals, as explained below.

7.4.3 The NDB Scheme provides three options for notifying affected individuals of the statement provided to the Information Commissioner:

a. Option 1: notify all individuals whose personal information was part of the EDB;
b. Option 2: notify only those individuals at risk of serious harm from the EDB; or
c. Option 3: if neither option 1 or 2 are practicable, the School must publish a copy of the statement provided to the Information Commissioner on its website if it has one and take reasonable steps to publicise the contents of the statement.

7.4.4 A School can use any reasonable method to notify individuals via option 1 or 2 (eg telephone call, SMS, physical mail, social media post, or in-person conversation), or their usual method of communicating with that individual.

7.4.5 Where the individual being notified is a pupil, it may be appropriate to notify the parent or guardian instead of or as well as the pupil. The age and maturity of the pupil will be an important factor when considering who to notify. This issue is discussed more fully in relation to consent and young people in Section 17.

7.4.6 Schools can tailor the notification to individuals, as long as it includes the content of the statement Schools must provide to the Information Commissioner. The NDB Scheme required the statement and the notification to individuals to include:

a. the identity and contact details of the School;
b. a description of the EDB and the organisation (eg the School) that has reasonable grounds to believe the EDB has happened;
c. the kind, or kinds, or information concerned;
d. recommendations about the steps that individuals should take in response to the EDB.

7.4.7 There are limited relevant exceptions to Schools' obligations to notify the Information Commissioner and/or individuals. These are:

a. if the EDB affects the security of personal information held by both the school and other organisations, only one organisation needs to prepare the statement and give notification of the EDB, for all affected organisations to comply with the notification requirements under the NDB Scheme; and
b. where the Information Commissioner makes a declaration that an entity is not required to comply with the notification requirements under the NDB Scheme or can delay giving notice. This declaration can be made as a result of a submission by the School about reasons why notification to Information Commissioner or some or all of the individuals should not be made or delayed.

7.4.8 Whilst not mandatory, in some circumstances it may be appropriate to also notify third parties such as:

a. Police or law enforcement – if theft of other crime is suspected – it can be an offence not to notify an indictable offence to the police;
b. Credit card companies or financial institutions – eg if the School or a service providers have obligations under other regulatory schemes such as credit card payment processors who are subject to the Payment Card Industry Security Standards or their assistance is necessary for contacting individuals or mitigating harm;
c. other internal or external parties not already notified – if they may be impacted by the EDB (eg professional bodies, or the ATO if Tax File Numbers are affected); and
d. the Australian Cyber Security agencies such as the ACS Centre, including National Computer Emergency Response Team (**CERT**) or the Australian Cyber Crime Online Reporting Network (**ACORN**) – if the School has been a victim of cyber-crime.They can offer further advice and support in relation to cyber security incidents and a report can be lodged and followed up by the appropriate agency.

12.5. Reviewing the Data Breach/EDB

7.5.1 Whether the incident that occurs is a Data Breach or an EDB that requires notification under the NDB Scheme, conducting a follow up review of the Data Breach once the above steps have been taken is very important so that Schools take action to prevent future breaches and ensure ongoing compliance with their data security obligations and overarching obligation to manage the personal information they hold in a compliant manner. This includes:

a. investigating and understanding the cause(s) of the Data Breach or EDB;
b. developing a prevention plan and conducting audits to ensure the plan is implemented;
c. considering changes to policies and procedures; and
d. further staff training staff.

12.6. Consequences

7.6.1 The NDB Scheme is subject to the existing regulatory and enforcement framework overseen by the Information Commissioner as set out in the Privacy Act. This means that the consequences of a School breaching a requirement of the NDB Scheme, include:

a. an investigation by the Information Commissioner into the causes of the Data Breach/EDB and the School's response;
b. a determination by the Information Commissioner that the School take specified steps to remedy noncompliance, perform any reasonable act to redress any loss suffered, pay monetary compensation;
c. a request that the School provide an enforceable undertaking that it will take, or refrain from taking, specified action. In the case of serious or repeated noncompliance; or

d. an application by the Information Commissioner to court to impose a civil pecuniary penalty of up to $2.1 million per breach.

12.7. Voluntary notification

7.7.1 Even when the Data Breach is not an EDB under the NDB Scheme, there may be instances where a School considers it necessary to voluntarily notify one or some affected individuals and the Information Commissioner of a Data Breach, in accordance with its obligations under APP11 to take reasonable steps to keep the personal information it holds secure (see Section 14) as well as for managing the reputational impact to the School and complying with its duty of care obligations.

13. Enquiries and Complaints

If you would like further information about the way the school or *the Schools' Company* manages the personal information it holds, or wish to complain that you believe that the school or *the School's Company* has breached the Australian Privacy Principles, please contact the school's Principal. The school or *the School's Company* will investigate any complaint and will notify you of a decision in relation to your complaint as soon as is practicable after it has been made.

Schools are required to advise individuals in their collection statement that their Privacy Policy contains this information.

14. Appendix A - Summary

1. DO, if asked, inform people about the type of personal information that is being collected about them and why.
2. DO encourage staff members to read the School's Privacy Policy.
3. DO make the Privacy Policy easily accessible.
4. DO ensure that the School's requirements in relation to collection, use and disclosure of personal information are followed.
5. DO ensure staff refer all queries about the Privacy Policy to the School's privacy officer.
6. DO consider how, and in what form, you store personal information, and consider how secure this is.
7. DO only collect personal information that the School requires to carry out its functions and activities.
8. DO identify the School and its contact details when collecting personal information.
9. DO inform individuals that they can access their personal information, subject to the requirements of the Privacy Act.
10. DO inform individuals of any plans to disclose their personal information to others.
11. DO consider, and notify individuals of, all the reasons for which you are collecting their personal information.
12. DO take reasonable steps to ensure that, when collecting personal information, individuals are made aware of the following matters unless it is obvious or they would already know:
    a. the School's identity and contact details;
    b. if the individual may not be aware that the information has been collected, the fact that it has been collected and the circumstances of the collection;
    c. if collected under or authorised by law, the fact that the collection is so required or authorised (including details of the law requiring or authorising collection);
    d. why the information is being collected;
    e. the main consequences (if any) if the individual does not disclose all or part of the information;
    f. any other entities or types of entities to whom the information may be disclosed;
    g. that the School Privacy Policy contains information about how an individual can access and seek correction of information;
    h. that the School Privacy Policy sets out how an individual may complain about a breach of their privacy and how the complaint may be dealt with; and if practicable to specify.
13. DO only use sensitive information for the purposes for which it was disclosed.
14. DO obtain consent if you collect sensitive information unless an exception applies.
15. DO make a written note of use or disclosure of personal information if used or disclosed under an exception in APP 6.2.
16. DO use or disclose an individual's personal information which is first collected by a related School only for the same primary purpose or reasonably expected related secondary purpose of collection of the related School.
17. DO take care when disclosing information overseas.
18. DO investigate the privacy obligations of overseas recipients of personal information, rather than simply taking their word for it, if you intend to rely upon the Reasonable Belief Defence. Do this by reviewing their privacy policy and terms and conditions of service/use.
19. DO ensure that 'cloud' providers provide appropriate undertakings, warranties and indemnities.
20. DO advise people if their information will or may be sent offshore and if practicable where it will be sent.
21. DO obtain consents for one-off transfers of information where it is practicable to do so.
22. DO only use identifiers which are created by the School to identify individuals, not GRIs.
23. DO, when passing personal information internally or to a related School, notify the other party of the age of the information if this is likely to affect its accuracy and currency.
24. DO consider the impact if the information is incomplete, inaccurate or out-of-date (eg. health information) and take appropriate steps.
25. DO investigate any clear inconsistencies with personal information held (eg. recorded as a male, but is an ex-pupil in an all girl school).
26. DO consider whether the information was collected directly from the individual and whether it is a reliable source.
27. DO give the individual a chance to comment on the information provided, if reasonable and practicable to do so.
28. DO, where practicable, check personal information with existing records collected for the same or a related purpose to see whether it is consistent, accurate and up-to-date before using or disclosing personal information.
29. DO try to provide individuals with user friendly ways to update their information.
30. DO keep records accurate by notifying a related School from/to which personal information is collected/disclosed of any changes to the information, and keep a record for such notification.
31. DO check with a person to whom information is to be disclosed about the purpose of the disclosure, if this is not clear.
32. DO be familiar with the School's systems to ensure accurate and up-to-date personal information is kept.
33. DO consider the age of personal information, and whether the information is likely to change (eg. an address is more likely to change rather than a name), in determining whether it is likely that the information is inaccurate, incomplete or out-of-date.
34. DO ensure that all hard-copy records of personal information are kept securely locked or supervised.
35. DO locate personal information that is no longer needed. In such cases, the information should be destroyed or de-identified.
36. DO ensure that staff maintain adequate security of all personal information under their control.

37. DO limit access to personal information only to those who require it to carry out their duties for a permitted purpose (ie. a 'need to know' basis).
38. DO contact the School's privacy officer if you are unsure as to the company's practices and procedures for keeping personal information secure.
39. DO make a note of to whom personal information has been disclosed, for example, a record of who has a particular file, or who has access to a particular database.
40. DO scrutinise requests for disclosure of personal information, for example follow the School's procedure to identify an individual who asks you to disclose or 'check' their personal information.
41. DO ensure that in cases of shared computers, tools are implemented to avoid possible privacy breaches.
42. DO ensure that staff log in and out in accordance with allocated level of access.
43. DO establish procedures for the destruction or de-identification of personal information which is no longer required.
44. DO consider the following matters when engaging a cloud service provider:
    a. the sensitivity of the data from a privacy perspective;
    b. the sensitivity of the data from a business operational perspective;
    c. in what jurisdictions may the data be stored by the cloud provider;
    d. is the data encrypted when transferred and stored; and
    e. what other forms of security does the provider use.
45. DO ensure the cloud service provider is subject to strict contractual provisions regarding security of the data and liability for any breach.
46. DO assess the information you use and disclose, and correct it if necessary to ensure it is accurate, up-to-date, complete, relevant and not misleading.
47. DO consider what steps are reasonable in the circumstances to correct information upon request by the individual.
48. DO encourage individuals to notify the School if they consider the personal information held about them is inaccurate, out-of-date, incomplete, irrelevant or misleading.
49. DO inform people of their right to correct their information. This must be done when collecting personal information.
50. DON'T collect personal information from someone about another individual (eg. next of kin details) unless it is unreasonable or impracticable for you to contact the individual directly.
51. DON'T collect unsolicited information if it is not reasonably necessary for a function or activity of the School whether information is likely to be disclosed overseas and, if so, to which countries,
52. DON'T collect sensitive information unless it is necessary.
53. DON'T use or disclose personal information unless with consent, for the primary purpose of collection or for a reasonably expected related secondary purpose of collection (or directly related secondary purpose in the case of sensitive information) or where another exception applies, such as exercising duty of care.
54. DON'T create databases that allow an individual's GRI to be entered in order to retrieve a record about the individual.
55. DON'T leverage off GRIs as a means of tracking students throughout their schooling life.
56. DON'T use or disclose GRIs unless it is necessary to fulfil an obligation to a government agency or authority, it is required or authorised by law, or it is necessary to verify a person's identity. An individual's TFN should never be used as an identifier.
57. DON'T continue to use information you believe to be out of date or inaccurate.
58. DON'T access, discuss, display, or disclose personal information other than as permitted by the APPs.
59. DON'T leave personal information unattended and not specially secure. For example, if staff leave their computers for an extended period of time, it should be shut down or they should log off or use a screensaver with password. Don't leave files where they may be accessed by unauthorised people.
60. DON'T ever allow unauthorised access, modification or disclosure of personal information.
61. DON'T refuse to correct personal information just because it may be costly, inconvenient or difficult to do so.

Version	Date	Comment
Current Version (v. 1)	**Aug 18, 2019 11:23**	**Bree Hills**