St John's Lutheran School, Kingaroy

Protection of Personal Information Policy

(April 2023)

GUIDING SCRIPTURE

Whoever derides their neighbour has no sense, but the one who has understanding holds their tongue. A gossip betrays a confidence, but a trustworthy person keeps a secret. (Proverbs 11: 12-13)

PURPOSE

The *Privacy Act 1988 (Cth)* sets out 13 *Australian Privacy Principles* which set out standards, rights and obligations in relation to collecting, storing, providing access to, using and disclosing personal information. This policy outlines the processes for dealing with personal information in accordance with privacy legislation.

SCOPE

The scope of this policy has application for all activities and personnel (including School Council members, staff, and contractors) involved with the collection, storage, use and disclosure of personal information. It also has application for any person/s the School collects, stores, uses or discloses personal information from.

DEFINITIONS

Definitions provided from the Privacy Act 1988.

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 of personal information collected by the School include an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details.

Sensitive information means information or opinion about an individual's racial or ethnic origin, political opinions or membership of a political association, religious beliefs or affiliations, 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, genetic information and biometric information about an individual.

POLICY STATEMENT

St John's Lutheran School respects the privacy of all individuals and believe any personal information collected by us or provided to us should be safely and securely held and used only for the purposes intended and agreed. St John's Lutheran School will take all reasonable measures to protect the privacy of individuals' personal information and to comply with the obligations imposed by the *Privacy Act 1988 (Cth)* and the *Australian Privacy Principles* (APPs).

PROCEDURES

1. Open and Transparent Management of Personal Information

St John's Lutheran School will maintain a clearly expressed and up to date *Privacy Policy* about the management of personal information. The School will ensure that the *Privacy Policy* is readily available free of charge and in an easy to read and appropriate format. The policy will be available to the public on our website and on request from our administration staff.

St John's Lutheran School will manage all personal information held by the School in an open and transparent way and will take all reasonable steps to ensure practices, procedures and systems comply with the APP's. Relevant staff will be informed about the handling of personal information and privacy compliance.

2. Collection of Personal Information

St John's Lutheran School collects personal information from individuals and third parties during the course of providing education services. St John's Lutheran School will only collect personal information (other than sensitive information) that is reasonably necessary for one or more of our functions or activities.

Unless an exception applies (as outlined in APP 3.4), St John's Lutheran School will only collect sensitive information about an individual where:

- The individual consents to the collection of the information. This can be express consent (orally or in writing) or implied consent (consent may be reasonably inferred in the circumstances);
- The information is reasonably necessary for one or more functions or activities.

  Exceptions include, but are not limited to, a permitted general situation exists such as lessening or preventing a serious threat to life, health or safety or taking appropriate action in relation to suspected unlawful activity or serious misconduct, locating a person reported as missing. Refer to APP 3.4 for more details.

Personal information will be collected in a way which is lawful and fair. St John's Lutheran School will collect personal information directly from the individual rather than from a third party unless it is unreasonable or impracticable to collect the personal information directly from the individual.

If information is not relevant or useful, St John's Lutheran School should not retain the information in its records. Instead of keeping a full copy of documents, the school will consider:

- Noting the information needed from a document then returning the document;
- Blanking out irrelevant parts of the document when copying it;
- If using a document to identify a person, make a note that the document has been sighted, including the date it was sighted, rather than keeping a copy.

2.1 Dealing with Unsolicited Information

Unsolicited information is information received without asking. If unsolicited personal information is received, and such information is not reasonably necessary or directly related to St John's Lutheran School functions or activities and the school could not have collected the information, the information will be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so.

3. Notification of the Collection of Personal Information

St John's Lutheran School will maintain an up to date *Privacy Policy* and *Collection Notice* (contained in the *Privacy Policy*) which notifies individuals about matters relating to the collection of their personal information. This policy is available on the school website, with a hyperlink also found on the 'Contact Us' page of the website.

4. Use or Disclosure of Personal Information

St John's Lutheran School will only use or disclose personal information for a purpose for which it was collected (primary purpose) or for a secondary purpose if an exception applies. Under APP6, exceptions include, but are not limited to:

- The individual has consented to a secondary use or disclosure;
- The individual would reasonably expect the school to use or disclosure their personal information for the secondary purpose (which is related to the primary purpose of collection);
- A permitted general situation exists such as lessening or preventing a serious threat to life, health or safety or taking appropriate action in relation to suspected unlawful activity or serious misconduct, locating a person reported as missing.

Refer to APP 6.2 for more details on exceptions.

4.1 Sharing of Personal Information under the Domestic and Family Violence Protection Act 2012 (Qld)

Under the Domestic And Family Violence Protection Act 2012 (Qld) [Part 5A Information Sharing], the Principal of St John's Lutheran School is classified as a 'prescribed entity', which means they are able to share information, while protecting the confidentiality of the information, in certain situations in order to assess and manage domestic and family violence.

The safety, protection and wellbeing of people who fear or experience domestic violence, including children, are paramount. The Act identifies the following key principles specific to information sharing:

a) Whenever safe, possible and practical, a person's consent should be obtained before:
   - Providing, or planning to provide, a service to the person
   - Disclosing personal information about the person to someone else

b) Because the safety, protection and wellbeing of people who fear or experience domestic violence are paramount, their safety and protection takes precedence over the principle mentioned above in point (a);

c) Before sharing information about a person with someone else, the Principal should consider whether disclosing the information is likely to adversely affect the safety of the person or another person.

There are many circumstances where it is not safe, possible or practical to seek consent. The safety, protection and wellbeing of people who fear or experience domestic and family violence are paramount and **safety takes precedence over consent**.

Information may be shared without consent under the above Act in two key circumstances:

1. Assessing a domestic violence threat:

The Principal may give information to any other prescribed entity (e.g., Qld Police, Child Safety, Department of Health, public health/ hospital, ambulance etc) or specialist domestic and family violence service provider if they reasonably believe a person fears or is experiencing domestic violence; **and** giving the information may help the receiving entity assess whether there is a serious threat to the person's life, health or safety because of the domestic violence.

2. Responding to a serious domestic violence threat

The Principal may give information to any other prescribed entity, specialist domestic and family violence service provider or support service provider if they reasonably believe a person fears or is experiencing domestic violence; **and** giving the information may help the receiving entity to lessen or prevent a serious threat to the person's life, health or safety because of the domestic violence.

The Principal may use information given to them to the extent necessary to lessen or prevent a serious domestic violence threat, including by, but not limited to:

- Contacting, or attempting to contact, the person or another person involved in the domestic violence
- Offering to provide assistance or a service to the person or another person involved in the domestic violence.

Safety Implications to Consider when Sharing Information

The Principal must consider whether disclosing personal information is likely to adversely affect the safety of the person or another person. If the Principal determines the person's safety may be adversely affected by sharing the information, the information may still be shared but the Principal should take steps (such as safety planning or appropriate referral) to help mitigate any identified risks.

Further information and guidance can be found in the Domestic and Family Violence Information Sharing Guidelines.

4.2 Information Sharing under the Child Protection Act 1999 (Qld)

Under the *Child Protection Act 1999*, the Principal of St John's Lutheran School is not legally required to seek or obtain consent from the person they are sharing information about in certain situations. Children's safety, wellbeing and best interests must be prioritised over the protection of an individual's privacy, by enabling information to be shared without consent for particular purposes.

Under legislation, the Principal should obtain consent from parents and children unless it is not safe, possible and practical. What is safe, practical and possible will differ and depend on the circumstances of the child and the family and will need to be assessed by the Principal, in regard to the particular purpose for which the information is being shared.

Circumstances where people may not be informed, or their consent obtained about their personal information being shared include where seeking and obtaining consent could jeopardise the safety or wellbeing of a person. For example, where:

- Doing so may place someone at risk of harm
- It is impracticable or impossible to contact a parent or a young person and the matter requires an urgent response
- There:
    - is a threat that a family may go into hiding or abduct a child
    - are assaults or threats to assault others
    - are attempts or threatened suicide
    - are concerns a child or another person could be coached or coerced.

St John's Lutheran School staff will follow the reporting procedures outlined in *#1.10 Child Protection Policy* when responding to harm, or allegations of harm, to students.

Further information can be accessed through Child Protection Act 1999 (Qld), Chapter 5A and Part 4 and the Department of Child Safety, Youth and Women Information Sharing Guidelines.

5. Direct Marketing

St John's Lutheran School will only use or disclose personal information (not including sensitive information) about an individual for direct marketing if the individual would expect the school to use information for that purpose. A simple 'opt out' mechanism is available for individuals to request not to receive direct marketing, and the individual has not made such a request. An individual may request at any time not to receive direct marketing information from the school by contacting administration.

6. Quality of Personal Information

St John's Lutheran School will take reasonable steps to ensure that personal information it collects is accurate, up to date and complete. Before using or disclosing personal information, the school will also take reasonable steps to check the information is accurate, up to date, complete and relevant.

Reasonable steps taken by the school include:

- Implementing internal procedures and systems to audit, monitor, identify and correct poor quality personal information, including training staff in these procedures;
- Implementing protocols that ensure personal information is collected and recorded in a consistent format;
- Ensuring updated or new personal information is promptly added to relevant existing records;
- Update personal information of students/parents annually.

7. Security of Personal Information

St John's Lutheran School will take reasonable steps to protect personal information from misuse, interference and loss, unauthorised access, modification or disclosure. Reasonable steps adopted by the school include:

7.1 Governance, Culture and Training

Privacy and security arrangements include appropriate training, resourcing and management focus to foster a privacy and security aware culture among staff and ensure they are aware of and understand their privacy and security obligations and the importance of good information handling and security practices. Governance arrangements in relation to personal information include risk management strategies.

The school has established clear procedures for oversight, accountability and lines of authority for decisions regarding personal information security, with the senior leadership team responsible for personal information, where and how it is held and for ensuring that it is held securely.

7.2 ICT Security

The school has appropriate and effective ICT security measures in place to ensue both hardware and software are protected from misuse, interference, loss, unauthorised access, modification and disclosure, whilst ensuring they remain accessible and useful to authorised users. Procedures are outlined in *#3.06 Information and Communication Technology Security Policy*.

7.3 Access and Physical Security

Access security and monitoring controls assist St John's Lutheran School to protect against internal and external risks by ensuring that personal information is only accessed by authorised persons. Internal access to personal information is limited to those who require access to do their job. Any information which is not considered relevant information will be not accessible to those staff. The electronic information management systems have inbuilt security features allowing access only to certain staff, with an audit function to review staff access. Processes are in place to identify individuals accessing systems, with access controlled by associating user rights and restrictions with their identity.

Physical security is an important part of ensuring that personal information is not inappropriately accessed, with measures in place which include:

- Cabinets which hold personal information are locked, with only authorised staff having key access;
- Building security alarm systems to detect unauthorised access to the building;
- Personal information is kept out of view and access to the public or unauthorised staff, with information not left exposed in reception;
- Reception staff are aware that conversations in the main reception area can often be overheard and as such, staff should avoid discussing confidential and sensitive information in this area.

Security measures are in place for information stored electronically, as outlined in *#3.06 Information and Communication Technology Security Policy.*

7.4 Destruction and De-Identification of Personal Information

Where St John's Lutheran School no longer needs personal information for any purpose for which the information may be used or disclosed, reasonable steps will be taken to destroy the information or ensure it is de-identified, except where the school is required by or under legislation to retain the personal information.

Where personal information needs to be destroyed or de-identified, the school will take reasonable steps to destroy or de-identify all copies it holds of the personal information, including copies that have been archived or are held as back-ups. Information will be disposed of in a manner that preserves the confidentiality of the person to whom the information relates. Reasonable steps taken by the school include:

- Hard copy information will be destroyed through a process of shredding prior to disposal;
- Information in electronic form will be 'sanitised' to completely remove stored personal information where it is possible. For hardware that cannot be sanitised, reasonable steps will be taken to irretrievably destroy it;
- Personal information stored by a third party such as cloud storage will require verification from the third party that secure destruction of this information has occurred;
- The Systems Administrator will ensure that back-ups of personal information are also destroyed or 'put beyond use';
- Equipment including computers, photocopiers and fax machines may have hard drive memory and confidential information will be properly removed prior to disposal of this equipment.

8. Access to Personal Information

8.1 Procedure for Providing Access

Where St John's Lutheran School holds personal information about an individual, we must, on request, give that individual (or their legal guardian) access to the information, unless a law allows for refusal (refer to *Section 8.2 Refusing Access to Personal Information*).

Requests must be made in writing to the Principal, who may discuss the need with the Chairperson of the School Council if and where necessary.

Prior to granting access to personal information, the Principal must be satisfied that a request for access to personal information is made by the individual concerned, or by another person who is authorised to make a request on their behalf (e.g., legal guardian). Where the individual is not known or readily identifiable to the Principal, personal identification such as a driver's licence should be sighted.

As archived files may have to be retrieved, the Principal or delegate will notify the individual or their legal representative of the anticipated length of time required before their personal information can be made available (generally within 30 days from the date of the request), and a day and time for access arranged with the individual.

The school will respond to the request for access to personal information within a reasonable period after the request is made and give access to the information in the manner requested by the individual (i.e., email, phone, in person, hard copy, or electronic), if it is reasonable and practicable to do so. Factors the school will consider when assessing what manner to provide the information include the volume of information requested, the nature of the information requested, and any special needs of the individual requesting the information.

Giving access to personal information may incur costs to the school for retrieval from archive storage. Should this be the case, a fee may be charged for the provision of information, however the fee will not be excessive. Where access fees are to be applied, the individual will be informed as soon as possible after submitting the request for access.

The Principal or delegate is responsible for reviewing the contents of any requested personal information and ensuring that any content falling within the exemption provisions is deleted using a black felt marker to cross out the exempt or irrelevant entries. These include any entries which could identify another individual, or which could have an adverse effect on the school's operations or activities.

Where access to personal information is to be accessed onsite, the individual and/or representative will be provided with a private area to access their personal file and will be accompanied by the Principal or delegated staff member, so that clarification of file entries may be given. Individuals may challenge information that they feel is incorrect. If information is established to be incorrect, it shall be corrected.

8.2 Refusing Access to Personal Information

Under the *Privacy Act 1988*, St John's Lutheran School is not required to give an individual access to personal information on the following grounds:

- The school reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- Giving access would have an unreasonable impact on the privacy of other individuals; or
- The request for access is frivolous or vexatious; or
- The information relates to existing or anticipated legal proceedings between the school and the individual, and would not be accessible by the process of discovery in those proceedings; or
- Giving access would reveal the intentions of the school in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- Giving access would be unlawful; or
- Denying access is required or authorised by or under an Australian law or a court/tribunal order; or
- The school has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the school's functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- Giving access would reveal evaluative information generated within the school in connection with a commercially sensitive decision-making process.

If St John's Lutheran School refuses to give access to personal information, they will provide written notification as to the reasons for the refusal and the complaint mechanisms available to the individual.

8.3 Access by Employees to Employee Records

As a private sector employer, St John's Lutheran School is exempt from the *Privacy Act 1988* in handling employee records if it is directly related to a current or past employment relationship. The school does not, therefore, have to grant an employee access to their employment record under the *Privacy Act*. The *Privacy*

Act only applies to an employee record if the information is used for a purpose not directly related to the employment relationship. However, workplace laws require a range of information to be made and kept for each employee. Employees or former employees can request access to these records under workplace laws or a court order. Further information can be found from the Fair Work Ombudsman.

9. Correction of Personal Information

St John's Lutheran School will take reasonable steps to correct personal information held to ensure that it is accurate, up to date, complete, relevant and not misleading, having regard to the purpose for which it is held. This applies to where the school believes the information is incorrect, out of date, incomplete, irrelevant or misleading or where an individual requests the school to correct their personal information.

Where St John's believes that personal information it holds may be incorrect, we will endeavour to confirm that the information is incorrect before correcting it. Where there is a disagreement about whether the information is indeed correct, the school will attach a statement to the original record outlining the individuals' claims.

The school will endeavour to determine that the request to correct personal information is made by the individual concerned, or by another person who is authorised to make a request on their behalf (e.g., a legal guardian).

The school will respond within a reasonable timeframe (preferably within 30 calendar days) after the request to correct personal information is made. The school will respond by correcting the personal information as requested by the individual, or by notifying the individual of its refusal to correct it.

10. Data Breach Response and Reporting

St John's Lutheran School has an obligation under the Notifiable Data Breaches Scheme to notify individuals and the Office of the Australian Information Commissioner about eligible data breaches.

10.1 Identifying an Eligible Data Breach

An eligible data breach arises when the following three criteria are satisfied:

1. There is *unauthorised access* to or *unauthorised disclosure* of personal information, or a *loss* of personal information, that the school holds (e.g., a device containing clients' personal information is lost or stolen; a database containing personal information is hacked; personal information is mistakenly provided to the wrong person); and
2. This is likely to result in *serious harm* to one or more individuals; and
3. The school has not been able to prevent the likely risk of serious harm with remedial action.

Unauthorised access of personal information occurs when personal information that the school holds is accessed by someone who is not permitted to have access (including employees, contractors or external third parties).

Unauthorised disclosure occurs when the school, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the organisation, and releases that information from its effective control in a way that is not permitted under the *Privacy Act*.

Loss refers to the accidental or inadvertent loss of personal information held by the school in circumstances where it is likely to result in unauthorised access or disclosure (e.g., employee leaves unsecured laptop containing personal information on public transport).

Serious harm to an individual may include physical, psychological, emotional, financial or reputational.

Refer to https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches for guidance on deciding whether an eligible data breach has occurred.

10.2 Responding to a Known or Suspected Data Breach

When St John's Lutheran School suspects that an eligible data breach may have occurred, staff must quickly assess the incident to determine if it is likely to result in serious harm to any individual.

Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and organisations. Hence, there will be no single way of responding to a data breach, but rather, each breach will be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

Generally, the actions taken following a data breach will include the steps outlined in the flowchart in Appendix 1 Action to Take After a Data Breach.

Further information can be found at:

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach

https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#notifying-individuals-about-an-eligible-data-breach and

https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#what-to-include-in-an-eligible-data-breach-statement

St John's Lutheran School must prepare and give a copy of the statement to the Commissioner as soon as practicable after becoming aware of an eligible data breach, ensuring all required information is included in the statement. The statement can be lodged to the Commissioner through an online form:

https://forms.uat.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

10.3 Other Considerations of a Data Breach

Where a known eligible data breach has occurred, the Principal will consider notification to the School Council. Where theft or criminal activity is suspected, the Principal is to notify the Police.

11. Video Camera Surveillance

11.1 Need for Video Camera Surveillance

St John's Lutheran School has installed video camera surveillance as an effective part of our risk management strategy to help the school to meet its obligations to provide a safe and secure environment for staff and students and meet its duty of care obligations.

In deciding on this strategy, the school considered:

- Past security incidents, issues and problems;
- How surveillance would assist;
- If there were any available alternative strategies to using surveillance that would achieve the intended purpose.

11.2 Purpose of Video Camera Surveillance

The school has implemented the use of video camera surveillance on the school grounds for the purpose of security and safety after school hours and, where appropriate, to provide an additional avenue for monitoring any behaviour or other incidents in the school grounds during school hours.

St John's Lutheran School has implemented strict practices associated with the operation of video camera surveillance, and the management of information collected through its use. The school has addressed privacy considerations of using this surveillance, which may involve the collection of personal information, to ensure compliance with the *Privacy Act 1988* and ensure consistency in decision-making and operational practices.

11.3 Collection of Surveillance Footage

Due consideration must be given to the location, position, angle and technical specifications of cameras to ensure the camera only collects necessary and relevant personal information in a way that does not unreasonably intrude into someone's personal affairs. They are to be located and positioned so that they

only view areas relevant to the intended purposes and the images captured enable identification of individuals for the intended purpose.

Surveillance must **not** be used for monitoring:

- Toilets
- Change rooms
- Classrooms
- Staff rooms and offices.

Video camera surveillance equipment is currently installed in the following locations:

- Administration entry
- Hall rear
- Undercover area
- Oval 1
- L Block courtyard
- Uniform shop
- K Block rear
- Administration rear
- Hall play area
- Tuckshop
- Oval 2
- H Block
- Bus pickup
- Carpark
- Grounds persons shed
- Library
- West playground
- Back entrance
- K Block

Additional locations and positioning of cameras will be made by the Principal on a case-by-case basis.

Surveillance footage must be image only, with no sound recording.

Video camera surveillance must not be used to covertly monitor staff under any circumstances. Staff need to be made aware of any areas that are captured by cameras, through the use of approved signage and information provided during induction or when there are changes to camera locations.

Appropriate signage must be placed at every entry point (gate/ entrance) to the school making the public aware of the video surveillance in use.

11.4 Safeguards Against Misuse of Personal Information

All stored video camera surveillance footage, and areas where monitoring of camera surveillance takes place is protected to ensure against misuse, loss and unauthorised access.

The control room is situated in the Archive Room located in the Administration Block. Physical safeguards are in place, with access to this room controlled by Grand Master level key access only. Stored digital footage is safeguarded using password protection to manage staff access.

Access to footage is limited to authorised staff for whom it is appropriate, being designated Administration, ICT staff and the Property Manager. The school will maintain an audit trail with every access event to be entered into the *Access Register* located next to the control panel.

Cameras are to be placed out of reach and in secure casing to safeguard access.

11.5 Deletion, Retention and Use of Recorded Footage

Personal information contained in video surveillance footage will only be kept for as long as necessary, and it will be disposed of appropriately to help protect the information from misuse, loss and unauthorised access, modification or disclosure.

Stored footage will be overwritten every 24 days as per the capability of our system.

Any footage deemed to be needed to be retained for a longer period of time will be stored on the hard drive of the controlling computer.

Footage will be used and disclosed in line with the school's requirements under the Privacy Act 1988, outlined in the *Section 4 Use or Disclosure of Personal Information*. The footage will only be used for the purpose for which it was obtained, unless an exception applies.

Any disclosure of footage must be recorded in the *Access Register*.

Footage may be scrutinised to ascertain details of any breach of security noted or any behavioural or other incident that may have occurred. Notes may be taken of what is viewed on the footage and time and location recorded in the *Access Register* to assist with any follow-up undertaken within the school.

If surveillance footage contains evidence relied upon in a decision to suspend or exclude a student, it must be retained for the same period of time the suspension/ exclusion documents are required to be retained. This is because the footage relied upon will form part of the decision to suspend or exclude the student.

Similarly, if surveillance footage is used to capture a workplace accident or personal injury giving rise to a personal injury or WorkCover claim, the footage must be retained for as long as the claim documents must be retained.

Surveillance footage may be used or disclosed for the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities to the Queensland Police Service or other enforcement body. The school must have a 'reasonable belief' that the use or disclosure is 'reasonably necessary'.

11.6 Access to Recorded Footage

Access to personal information obtained through video camera surveillance footage will be in line with the procedures outlined in the *Section 8 Access to Personal Information.*

In summary:

- Access must be in writing to the Principal;
- Access will only be granted to the individual concerned or another person who is authorised to make such a request on their behalf (e.g. parent or legal guardian);
- The Principal or delegate is responsible for reviewing the contents of any requested personal information. The school reserves its right to allow or refuse access on certain grounds (refer to *Section 8.2 Refusing Access to Personal Information).* Such requests will be considered on a case-by-case basis;
- Where there are other identifiable people in the footage other than the person requesting access, the school may deny access;

Access to personal information footage recorded through video surveillance will be recorded on the Access Register.

Security measures are to be implemented to ensure disclosed recorded footage is safely conveyed to the required party and subsequently destroyed after use or returned to the school.

Communication of Policy	The St John's Lutheran School *Protection of Personal Information Policy* will be available for staff on the school intranet.
Legislation / References:	• Child Protection Act 1999 (Qld) • Criminal Code 1899 • Domestic and Family Violence Protection Act 2012 (Qld) • Education (General Provisions) Act 2006 • Privacy Act 1988 (Cth)
Changes to this Policy from Version 2.0	Section 10.2 Responding to a Known/Suspected Data Breach: additional wording around the schools immediate response

Appendix 1: Action to Take After a Data Breach