POL04 DATA BREACH RESPONSE

RATIONALE	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. A response plan is required to enable Trinity Lutheran College to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals.
SCOPE	This policy applies to all members of the College community including staff, students, parents and other external stakeholders.
RESPONSIBILITY	The Principal has overall responsibility for this policy, which is administered by the Privacy Officer.
DEFINITIONS	**Personal information** is any information or opinion (whether true or not) which either identifies a person or from which a person's identity can reasonably be determined. Personal information can only relate to human beings. Information about companies and other legal entities is not covered by the provisions of the Privacy Act. **Sensitive information** is personal information that includes information about: • racial or ethnic origin • political opinions • sexual preferences or practices • criminal record • health This sort of information has extra protection under the law. **OAIC** – Office of the Australian Information Commissioner **DBRT** – Data Breach Response Team
POLICY	**A. OVERVIEW** This data breach response plan (response plan) sets out procedures and clear lines of authority for Trinity Lutheran College staff in the event that Trinity Lutheran College experiences a data breach (or suspects that a data breach has occurred). It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist the OAIC to respond to a data breach. **B. PERSONAL INFORMATION HELD BY TRINITY LUTHERAN COLLEGE** The type of information Trinity Lutheran College collects and holds includes (but is not limited to) personal information, including sensitive information, about: • Staff members, job applicants, volunteers and contractors; • Students and parents/carers ('parents") during and after the course of a student's enrolment at a Trinity Lutheran College; • Other people who come into contact with Trinity Lutheran College. **C. WHEN SHOULD THE DATA BREACH BE ESCALATED TO THE TRINITY LUTHERAN COLLEGE DATA BREACH RESPONSE TEAM?** a. The Privacy Officer should use discretion in deciding whether to escalate to the response team. b. Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team.

For example, a Trinity Lutheran College employee may, as a result of human error, send 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 officer can contact the recipient and the recipient agrees to delete the email, it may be that there is no utility in escalating the issue to the response team.

c. In making a determination as to whether a data breach or suspected data breach requires escalation to the response team, the Privacy Officer should 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 Trinity Lutheran College processes or procedures?
   - Could there be media or stakeholder attention as a result of the breach or suspected breach?

d. If the answer to any of these questions is 'yes', then it may be appropriate for the Privacy Officer to notify the response team.

e. If the Privacy Officer decides not to escalate a minor data breach or suspected data breach to the response team for further action, they should report to the Principal and College Council the following information:
   - description of the breach or suspected breach
   - action taken by the Privacy Officer to address the breach or suspected breach
   - the outcome of that action and the Privacy Officer's view that no further action is required

f. A record of the above shall be electronically filed (site to be determined).

PROTOCOLS

1. FLOWCHART

TLC EXPERIENCES DATA BREACH/DATA BREACH SUSPECTED

- Discovered by TLC staff member or TLC otherwise alerted

WHAT SHOULD THE TLC STAFF MEMBER DO?

- Immediately notify the Privacy Officer of the suspected breach
- Record and advise the Privacy Officer of the time and date the suspected breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach

WHAT SHOULD THE PRIVACY OFFICER DO?

- Determine whether a data breach has or may have occurred.
- Determine whether the data breach is serious enough to escalate to the Data Breach Response Team (some breaches may be able to be dealt with at the Principal level).
- If so, immediately escalate to the Data Breach Response Team.

PRIVACY OFFICER CONVENES TLC DATA BREACH RESPONSE TEAM

AREA	INTERNAL	EXTERNAL
Legal & Records	Principal / Deputy / Business Manager	TASS / ISV / MOORES NFP
Information Technology & Digital Systems	IT Manager / Business Manager / Principal	Integrated Technology Mildura (INTEC)
Communications	Principal / Deputy	LEVNT / ISV

2. DATA BREACH RESPONSE TEAM CHECKLIST

a. Process

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected breach.

- **STEP 1**: **Contain the breach and do a preliminary assessment**
- **STEP 2: Evaluate the risks associated with the breach**
- **STEP 3**: **Notification**
- **STEP 4**: **Prevent future breaches**

The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

The response team should refer to the OAIC's *Data breach notification: a guide to handling personal information security breaches* which provides further detail on each step.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

In reconsidering Trinity Lutheran College's processes and procedures to reduce the risk of future breaches (Step 4), the response team should also refer to the OAIC's *Guide to securing personal information*. This guide presents a set of non-exhaustive steps and strategies that may be reasonable for Trinity Lutheran College to take in order to secure personal information, and considers actions that may be appropriate to help prevent further breaches following an investigation.

b. Records management

A record of all actions by the response team will use the Data Breach Action template. All associated documents will be filed together and held electronically (site to be determined).

c. Data Breach Response Team Checklist

STEP 1 Contain the breach and make		Convene a meeting of the data breach response team.
		Immediately contain breach: • IT to implement the ICT Incident Response Plan if necessary. • Building security to be alerted if necessary.

a preliminary assessment		Inform the Trinity Lutheran College Council, LEVNT Director Operations, and if so advised the Australian Privacy Commissioner. Provide ongoing updates on key developments.
		Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing Trinity Lutheran College to take appropriate corrective action.
		Consider developing a communications or media strategy to manage public expectations and media interest.
STEP 2 Evaluate the risks for individuals associated with the breach		Conduct 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 the affected individuals, or possible affected individuals • the risk of serious harm to the affected individuals • the risk of other harms.
		Determine whether the context of the information is important.
		Establish the cause and extent 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 steps taken to rectify the situation and the decisions made.
STEP 3 Consider breach 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 Trinity Lutheran College is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.
STEP 4 Review the incident and take action to prevent future breaches		Fully investigate the cause of the breach.
		Report to Trinity Lutheran College Council and LEVNT 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 effected.

RECORD OF IMPLEMENTATION

Contact officer	*Cheryl Bartel (Principal)*
Approved by	*Executive leadership March 2018*
Ratified by	*Trinity Lutheran College Council August 2018*
Authorization	*Trinity Lutheran College Council authorizes this policy for publication and implementation having considered relevant legislation and/or operational requirement of users.*
Tracking	*Ratified 21 August 2018*
Review Date (3 year cycle or as required by legislation)	*2021*