POLICY

Privacy Policy 3.33

RATIONALE

Privacy is everyone's responsibility. This policy applies to all Bethlehem College employees, board and committee members, and volunteers who may be required to collect, access, use or disclose personal information, who may manage projects or systems that impact on personal information management, or who are responsible for making policy decisions about the way Bethlehem College manages personal information.

Bethlehem College collects and processes personal information about students, parents, alumni, donors, staff members, suppliers, contractors, and individuals who visit its websites or campuses.

Bethlehem College recognises that the individuals it collects information about hold a reasonable expectation that their personal information will be treated with utmost care and respect. Bethlehem College operates with a Privacy Statement that outlines its commitment to ensuring the privacy of all personal information it holds.

This policy seeks to ensure:

- *Data minimisation* – limiting the amount of personal information Bethlehem College collects and retains.
- *Transparency* – being open and honest about what information Bethlehem College collects and how it will be used and disclosed.
- *Security* – protecting from harm all the personal information collected by Bethlehem College.
- *Use and disclosure limitation* – making sure Bethlehem College uses and discloses personal information only when necessary and with a lawful basis.
- *Privacy rights* – ensuring that those whose information is held by Bethlehem College understand their rights regarding their personal information.

POLICY STATEMENT

Bethlehem College will only solicit, collect, retain and disclose personal information that the College' needs for lawful purposes.

BIBLICAL PRINCIPLES

Proverbs 11:13	A gossip betrays a confidence, but a trustworthy person keeps a secret.
Proverbs 25:9b	..do not betray another's confidence.
Titus 2:7	In everything set them an example by doing what is good. In your teaching show integrity, seriousness.

Proverbs 12:23 The prudent keep their knowledge to themselves, but a fool's heart blurts out folly.

GUIDELINES

Collection

1. Where a process or system can operate without the collection of identifying information, an individual must be permitted to do so anonymously.

2. Personal information should be collected from individuals directly, unless the situation requires that the information be collected from a third party (e.g. guardian / parent of a student, transferring school).

3. At the time that personal information is being collected from an individual, the College must ensure that the collection is done in a way that is fair and does not intrude to an unreasonable extent upon the personal affairs of the individual concerned, and that individuals are made aware:

- what information is being collected
- why the information is being collected
- how the information will be used
- who the information will be shared with, and
- what rights they have to access and correct that information.

4. If the information collected is a routine part of Bethlehem College process (that is, the collection of information is not unusual or ad hoc), it will be sufficient for compliance with item 3 above if Bethlehem College refers or provides the individual with a link to the relevant Privacy Statement. Occasional or ad hoc collections, such as individual research projects, may require the provision of specific privacy notices relating to that collection.

5. Where a new collection, use or disclosure of personal information is to become a routine part of Bethlehem College's process, the Privacy Officer is to be notified.

Use and disclosure

6. Except as provided in item 7, personal information must only be used or disclosed by Bethlehem College if that use or disclosure is a purpose for which the information has been collected.

7. Before using or disclosing personal information in new ways, or in ways that are not part of the College' routine business, the College must ensure that this is necessary for a lawful purpose or is otherwise permitted or required by law.

Note: Usually the best way to use or disclose information in new ways is to seek the authorisation of the individual. If this is not practicable in the circumstances, Bethlehem College must be able to rely on an exception to Principle 10 (use) or Principle 11 (disclosure) of the Privacy Act 2020. If this is not clear, the Privacy Officer must be consulted.

8. Bethlehem College must take reasonable steps to ensure that personal information is accurate and up to date before using or disclosing it, particularly where this use or disclosure could impact on the rights or interests of the person to whom the information relates.

9. Before sharing personal information with a contracted service provider, or disclosing personal information to an overseas recipient (other than the individual to whom the information relates), Bethlehem College must ensure that:

- the service provider or recipient is required and able to provide an adequate level of protection to the personal information shared.
- that the individual to whom the information relates has consented if the personal information is to be disclosed to an overseas party in a jurisdiction that does not require protection in a way that, overall, provides comparable safeguards to those under the Privacy Act 2020.

Access and correction

10. Every individual, or their authorised representative, has the right to request access to the personal information Bethlehem College holds about them, or to ask for their personal information to be corrected if they think it is wrong.

Security and retention

11. Bethlehem College have a responsibility to protect the personal information they handle against loss, misuse, unauthorised access or disclosure, and modification.

12. Information security is an important part of good personal information management.

13. Bethlehem College must only access or use personal information – whether within an information system or in hard copy – when this is necessary for a legitimate purpose.

14. Bethlehem College must not retain personal information for longer than the College has a lawful purpose to retain or use it.

15. Bethlehem College must ensure that any privacy breach identified is reported promptly to the Privacy Officer in compliance with the Privacy Breach Response Plan.

Privacy impact assessments

16. Wherever possible, Bethlehem College endeavours to take a "privacy by design" approach to the development of new or changed processes or systems. This means that we adhere to the following principles:

- Proactive not reactive; preventative not remedial
- Privacy as the default
- Privacy embedded into design
- End-to-end security – lifecycle protection
- Visibility and transparency
- Respect for user privacy

17. All Bethlehem College staff members must:

- understand and comply with the Privacy policies and framework
- actively participate in any privacy training provided by College, and
- keep their Manager and/or the Privacy Officer informed of any personal requests for information, privacy breaches, and other privacy issues.

19. Managers must:

- support staff to understand and comply with this policy and participate in any privacy training provided by the College, and
- ensure personal requests for information, privacy breaches, and other privacy issues are identified and managed in accordance with the Privacy Framework.

20. The Privacy Officer is responsible for:

- supporting all Bethlehem College staff members to understand and comply with the Privacy policies and Framework, including maintaining and developing relevant procedures, standards and guidelines
- assisting with the management of personal requests for information, privacy breaches and other privacy issues by Bethlehem College staff members
- managing privacy complaints from individuals
- reporting on privacy breaches and general privacy compliance to the Board
- liaising with third parties in respect of privacy matters, including the Privacy Commissioner or other relevant regulators and individuals.

Definitions

The following definitions apply to this policy:

Individual means any natural person about whom Bethlehem College collects and holds personal information and includes students, parents / guardians, staff members, contractors, alumni and friends, donors, and visitors to the College websites or campuses.

Lawful purpose means a purpose that is directly connected with any of the College's lawful functions, and includes, but is not limited to: (i) considering applications for admission to, or employment with, Bethlehem College; (ii) administering programmes of study; (iii) managing staff and ensuring the health and safety of students and staff members; (iv) and meeting the College's reporting requirements.

Personal information means any information, whether electronic or hard copy, about an individual, whether or not the information directly identifies the individual, and includes but is not limited to contact, demographic, health and academic information (including course results), CCTV footage, staff performance information, emails and other correspondence, and opinions about the individual.

Privacy breach means an event (whether intentional or unintentional) in which personal information is lost, cannot be accessed as a result of an action, is accessed, altered, disclosed, or destroyed without authorisation, or is at increased risk due to poor security safeguards, including but not limited to:

- accidental disclosure of personal information to the wrong recipient;

- employee browsing of personal information without a legitimate reason;
- an attack on a Bethlehem College system; or
- a lost or stolen Bethlehem College device or document.

Privacy Framework means this policy and all plans, procedures, standards, statements, and guidelines issued to support it.

Bethlehem College includes members of the Christian Education Trust, committee members, staff members, students, board of trustee members, volunteers and contractors working for and on behalf of Bethlehem College and, for the purposes of the Privacy Framework , includes students who collect or process personal information in the course of their studies or research, or who are otherwise permitted access to personal information held by the College.

BETHLEHEM COLLEGE - PRIVACY STATEMENT

Bethlehem College may collect personal information from and about students, parents /guardians, employees, committee members, board members, volunteers, campus visitors, vlumni members, contractors, and suppliers including:

- name
- date of birth
- contact information
- location
- interactions with the College
- student enrolment, attendance, performance, and achievement information
- employment information
- billing, payment or purchase information

Bethlehem College collects, uses, and discloses this personal information to effectively and efficiently process financial transactions, enrol and educate students, meet curriculum requirements, record and maintain records of academic progress, report to parents, maintain the school-home partnership, provide access to services, enable discipline / behaviour management programmes, provide accurate information to other education providers to ensure proper and safe student transfers, celebrate success, maintain alumni records, market and promote Bethlehem College, maintain school websites and publications, manage staff, manage health and safety, and to ensure that all areas of operation of the College are in compliance with current legislation.

Staff of Bethlehem College have access to personal information collected within the areas of responsibility within their positions. Bethlehem College may share personal information that it holds for legitimate reasons.

Anyone has the right to ask for a copy of any personal information that Bethlehem College may hold about them, and to ask for it to be corrected if they think it is incorrect.

If a person would like to ask for a copy of their information or to have it corrected, they should contact Bethlehem College by emailing karen.miller@beth.school.nz or by telephoning 07 579 1800 or by sending a request by mail to the Privacy Officer (Larne Edmeades, Private Bag 12003, Tauranga, 3143.

BETHLEHEM COLLEGE - PRIVACY BREACH RESPONSE PLAN

RATIONALE

The purpose of this response plan is to ensure that privacy breaches are managed in accordance with the Bethlehem College privacy policy and in compliance with Bethlehem College's obligations under the Privacy Act 2020, including compliance with privacy breach notification requirements.

A privacy breach occurs when Bethlehem College intentionally or accidentally; (i) provides unauthorised or accidental access to someone's personal information; (ii) discloses, alters, loses, or destroys someone's personal information; (iii) loses access to personal information (such as through a hack or ransomware attack). Privacy breaches can cause harm to the individual to whom the information relates.

A privacy breach could also, if poorly managed, significantly damage Bethlehem College's reputation.

This plan follows the Privacy Commission's recommended best practice for responding to a privacy breach. These procedures are intended to ensure transparency and accountability, not blame. All members of Bethlehem College community should feel safe to speak up. Once alerted to a privacy breach, Bethlehem College can take steps to manage that breach.

The procedure requires speed, care, and collaboration. It is essential to include the right people at the right time. Responding as quickly and professionally as possible will help minimise any harm caused to the affected person/s and the College.

BIBLICAL PRINCIPLES

Colossians 3:23	Whatever you do, work at it with all your heart, as working for the Lord, not for human masters.
James 5:16	Therefore confess your sins to each other and pray for each other so that you may be healed. The prayer of a righteous person is powerful and effective.
1 John 1:7	But if we walk in the light, as he is in the light, we have fellowship with one another, and the blood of Jesus, his Son, purifies us from all sin.
Romans 12:16-18	Live in harmony with one another. Do not be proud but be willing to associate with people of low position. Do not be conceited. 17 Do not repay anyone evil for evil. Be careful to do what is right in the eyes of everyone. 18 If it is possible, as far as it depends on you, live at peace with everyone.

REPORTING A BREACH

1. Any member of the Bethlehem College team who causes or discovers a privacy breach must report the breach to their Head of School *as soon as practicable*.

2. That Head of School must then notify the Bethlehem College Privacy Officer as soon as practicable of the privacy breach.
3. The Privacy Officer will appoint someone to lead the response, which will be carried out in accordance with the Guidelines below.

GUIDELINES – HOW TO RESPOND TO A PRIVACY BREACH

There are four key steps in dealing with a privacy breach:

1. Contain
2. Assess
3. Notify
4. Prevent

Complete the first three steps either at the same time or in quick succession.

Use step four to determine longer-term solutions and prevention strategies.

Every privacy breach has a different level of risk and impact. Evaluate and respond to each incident on a case-by-case basis.

Step 1: Contain

Once a privacy breach is discovered, act quickly to contain it and then determine what went wrong.

Containment actions could include:

- trying to get lost information back
- disabling the breached system
- cancelling or changing computer access codes
- trying to fix any weaknesses in the organisation's physical or electronic security.

Step 2: Assess

Assessing the risks of the privacy breach will help determine the next steps.

The Privacy Commission has a self-assessment tool to determine the seriousness of the privacy breach called the Notify Us tool.

Consider the following elements of the breach:

The types of personal information involved

The more sensitive the information, the higher the risk of harm to the people affected. A combination of personal information is usually more sensitive than a single piece of personal information. Health information, driver licence numbers, and credit card details can all cause harm on their own, but together they could be used for identity theft.

What personal information might show

As an example, a list of customers on a newspaper delivery route may not be sensitive. But the same information about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

If the personal information is easy to access

If the information is not protected by a password or encryption, then there is a greater risk of someone misusing it.

The cause of the breach

Try and find out what caused the breach, and if there is a risk of further breaches.

The extent of the breach

Try and identify the size of the breach, including:

- how many people can access the lost information?
- how many people have lost personal information?
- the risk of the information being circulated further.
- whether the breach is the result of a systemic problem or an isolated incident.

The potential harm resulting from the breach

Think about this from the point of view of the people affected. Types of harm could include:

- identity theft
- financial loss
- loss of business or employment opportunities
- significant humiliation or loss of dignity

Each incident should be considered on a case-by-case basis. Also, think about:

- the risk of harm to people affected
- whether there's a risk of identity theft or fraud,
- whether there is a risk of physical harm
- whether there is a risk of humiliation, loss of dignity, or damage to the person's reputation or relationships. For example, if the lost information includes mental health, medical, or disciplinary records.
- What affected people can do to avoid or minimise possible harm, e.g., change a password
- whether a person have any legal or contractual obligations
- How sensitive is the information that is involved in the breach? Examples of sensitive information could be about someone's health, political or religious beliefs, or financial information. Context is important. Information that is not sensitive in one situation might be very sensitive in another.

Who holds the information now?

Information in the hands of people with unknown or malicious intentions can be of significant risk to the people affected.

The risk will be lower if the information went to a trusted person or organisation, and it is expected they would return it.

Warning: Be careful not to destroy evidence that the organisation or Police might need to assist them to find the cause of the problem or fix the issue.

Step 3: Notify.

Who should be notified?

Any person that could suffer harm as a result of Bethelhem College's privacy breach should be informed (unless an exception applies) about the breach to allow them to act to protect themselves. For instance, they may need to change their passwords or monitor their bank accounts for malicious activity.

If the consequences from the breach are minimal or minor, or if telling people would cause more worry and harm than not telling them, it may be acceptable not to tell the affected individuals.

It is not always necessary to notify people of a breach. If there's no risk of harm, advising may do more harm than good.

Mandatory privacy breach reporting

From 1 December 2020, the Privacy Act 2020 makes it a legal requirement to report privacy breaches that have caused serious harm or are likely to do so.

Use the Privacy Commission's online tool to help assess whether the breach is a serious one and report privacy breach: Notify Us Tool.

If unsure contact the Privacy Commission directly
Enquiries line: 0800 803 909 (Monday to Friday, 10:00am to 3:00pm).
https://www.privacy.org.nz/about-us/contact/

Notifying third parties

Consider any obligations of confidentiality and decide whether the following third parties should be informed:

- police (if the breach appears to involve theft or other criminal activity)
- insurers
- professional or other regulatory bodies
- credit card companies, financial institutions or credit reporting agencies
- third party contractors or other parties who the breach may affect
- internal business units
- the Bethlehem College board and the government minister
- union or other employee representatives.
- legal advisers

When to notify

If it decided to notify the affected person, do it as soon as reasonably possible. However, if law enforcement is involved, check with them first in case it compromises the police investigation.

How to notify affected people

The Entity that has a direct relationship with the person affected should be the one to notify them.

Be open and transparent with the affected people about how their personal information has been handled.

It's usually always best to notify the people affected directly, such as

- by phone
- by letter
- by email
- in person.

The affected people should only be notified indirectly (e.g., through website information, posted notices, or the media) if:

- telling them directly could cause further harm
- it's too expensive to notify them directly
- their contact details are not available.

Consider notifying vulnerable people through or with a support person.
It may be appropriate to notify people in more than one way.

What to say

The breach notifications should contain:

- information about the incident, including when it happened
- a description of the compromised personal information
- what the College is doing to control or reduce harm
- what the College is doing to help those that the breach affects
- what steps people can take to protect themselves
- contact information for enquiries and complaints
- offers of support when necessary, e.g. advice on changing passwords.
- whether the organisation has notified the Office of the Privacy Commissioner
- contact information for the Privacy Commissioner

Suggested guidelines for coping with media interest

For the Privacy Officer and/or Board Chairperson only

Note: Only the Privacy Officer and/or Board Chairperson are authorised to speak to the media.

How the College responds to media interest in the breach can be just as crucial to the College's reputation as the breach itself.

- Response to journalists quickly will show that the College is treating the incident seriously and not hiding from news coverage.
- Consider the messages carefully before delivering them.
    - Get the tone right.
    - Accept the blame and apologise if necessary.
    - Demonstrate empathy for those most affected by the breach.
    - Show that the wellbeing of those who may have been harmed is the organisation's highest priority.
- Feed the news cycle and keep journalists informed about what is happening.
- Media conferences can be an effective way of getting the organisation's response in front of the public.
- Monitor news media reports and social media about the incident.
- Address misinformation and disinformation and incorporate the College's responses into the broader communications and media strategy.
- Keep talking until the news story drops out of the news cycle and off the news agenda.

Step 4: Prevent.

The most effective way to prevent future breaches is to a well-thought-out security plan for all personal information.

In the aftermath of a breach, take the time to investigate the breach's cause and update the prevention plan.

Review the organisation's policies to minimise the collection and retention of personal information.

The effort put into an investigation should reflect the significance of the breach and whether it happened because of a systemic problem or an isolated event.

An investigation could include a:

- security audit of both physical and technical security
- review of policies and procedures
- review of employee training practices
- review of any service delivery partners caught up in the breach.

Review the improved prevention plan regularly to make sure it works and how the organisation is implementing it.

RELATED DOCUMENTS

The following documents set out further information relevant to this policy:

- Privacy Act 2020
- Health and Safety at Work Act 2015
- Human Rights Act 1993
- Crimes Act 1961