Privacy Policy

Purpose

This policy defines the way Kristin expects board members, staff, volunteers and contractors to handle personal information, including the way we collect, store, use and disclose this information. In addition to ensuring that we're complying with privacy laws and regulations, this policy is intended to support our values and the following underlying principles:

- We must manage personal information in accordance with our Christian values of progress, vision, integrity and love
- In doing so, we will maintain the trust and confidence of our students and community
- Privacy is not a barrier to legitimate information sharing, which is critical to delivering educational services and keeping people safe
- But, we must keep our students' best interests in mind when making data decisions

Please note, this **Privacy Policy** sets the rules for managing personal information at Kristin. The **Privacy Statement** and Student Privacy Statement that follow this policy explain to students and their parents how we manage personal information at Kristin.

Scope

This policy applies to:

- The actions of all board members, staff, volunteers, contractors, and any other people associated with Kristin, who may have access to the personal information we hold.
- The management of all personal information Kristin collects or generates about our students, alumni, wider community (parents, guardians and visitors), and staff, contractors and volunteers (note, the Kristin Privacy Statement document does not apply to information about staff, contractors and volunteers).

Personal information

Personal information means **any information about an *identifiable* individual**. To be personal information, the information:

- has to tell us something about a person; and
- has to identify a person, either because it includes a name or identifier (like a Student ID) or because it contains enough detail to reveal who they are; and
- could be in any form, including databases, spreadsheets, reports, letters, emails, file notes, phone recordings, location information, photographs and CCTV or video footage.

Roles and responsibilities

Role	Responsibility
Board of Governance	• Accountable for overall privacy compliance • Managing serious breaches of Privacy Policy
Executive Principal *Privacy Officer - Executive*	• Supporting Privacy Officer (Ops) and Principals & Directors to ensure compliance with Privacy Policy • Approval of significant departures from Privacy Policy • Sign-off on privacy breach notification • Liaison with Privacy Commissioner
Specialist Support *Privacy Officer - Operational*	• Assisting staff to understand and comply with Privacy Policy • Assisting with management of privacy issues • Providing privacy training to staff and volunteers • Escalating issues as required to the Privacy Officer (Exec)
Principals & Directors	• Ensuring their staff and volunteers comply with Privacy Policy • Ensuring department complies with Privacy Policy • Managing privacy issues and requests relating to department • Escalating issues as required to Privacy Officer (Ops) or (Exec)
Staff, contractors and volunteers	• Understanding and complying with Privacy Policy • Engaging with privacy training • Escalating privacy issues to Principals & Directors or Privacy Officer (Ops)

Our principled approach to privacy management

This policy cannot anticipate every scenario that might arise, so it takes a principled approach. If we follow the privacy principles, make common sense decisions that focus on student wellbeing, and escalate the difficult issues to our Privacy Officer, we will get it right.

Collecting personal information (Principles 1-4 of the Privacy Act)

- We should collect only the information **we really need** to do our jobs, run our school and deliver educational and pastoral services.
- We should collect information **directly from the people concerned** when we can. We can go to third parties (such as parents or families) to collect information if:
  - The person has authorised us to;
  - It would not be practicable to collect the information from the person (for example, if the person does not know the information); or
  - It would prejudice the purposes of collection (for example, if we're investigating a bullying incident).

- We must **tell people** what information we're collecting, why we need it, and how we will use or share it. Usually, it will be enough to direct people to our privacy statement (at the end of this policy). However, if we need to collect sensitive information or do something unexpected with it, then we may need to tell people specific things at the time of collection.
- We should collect information in ways that are **fair and not unreasonably intrusive**. This requires us to consider:
    - The **age** of the person we're collecting information from. The younger they are, the less they may understand about the consequences of giving us information or authorising us to collect it from someone else.
    - **Cultural or religious sensitivities** about sharing certain information. For example, gender differences could be more important for some cultures.
    - The **power imbalance** between a teacher and their student, or between school staff and parents or guardians, which can have an impact on fairness.
    - The **environment** within which we're collecting information. For example, we should not ask students to reveal sensitive information in a classroom setting.

Keeping personal information secure (Principles 5 and 9 of the Privacy Act)

- All staff, volunteers and contractors have a responsibility to protect the personal information they handle against loss, misuse, or unauthorised access, modification or disclosure.
- We should only access or use personal information – whether within an information system or in hard copy – if this is necessary for a legitimate business purpose connected with our role. This includes ensuring that volunteers only have access to the information they really need for the role they are performing for us.
- Personal information must be stored in the appropriate Kristin information systems. Where possible, staff should not duplicate information across multiple systems and must not retain information on their own desktops or devices.
- Staff should not use new third-party software, platforms, or web-based applications or ask students or parents to use these, without the approval of their line manager, in consultation with ICT and the Privacy Officer (Ops).
- Personal information must not be retained for longer than Kristin has a lawful purpose to use it.

Managing requests for information (Principles 6 and 7 of the Privacy Act)

- Staff, Students, alumni, parents/guardians (or their representatives) or any other individual have the right to request a copy of the information we hold about them (or to correct their information if they think it is wrong). We **must** release information on request, unless we have a lawful basis to withhold it.
- Parents/guardians can act as representatives for their children and, in practice, they usually will (particularly in relation to young children). We can release information about a student to their parent/guardian if we believe they are lawfully acting as a representative. However, if we have any reason to believe releasing the information would not be in the best interests of the student, we should refuse and escalate the request to a Principal or Director.
- We must process Privacy Act requests as quickly as possible, and respond no later than 20 working days after we receive them.
- We must escalate high-risk Privacy Act requests to a Principal, Director, or the Privacy Officer (Exec). High-risk requests are requests:
    - in which the requester specifically mentions the Privacy Act;
    - that relate to a legal or other dispute between the requester and Kristin;
    - that have been made by a lawyer on behalf of the requester; or
    - from parents or guardians, where we believe that releasing the information would not be in the best interests of the student.
- If we need to withhold information, we must tell the student or their representative why and inform them of their right to complain to the Privacy Commissioner. Decisions to withhold information should be made by a Principals or Directors or the Privacy Officer (Exec), and in consultation with the Board of Governance (which is ultimately responsible for the way we comply with the Privacy Act).

Using and sharing personal information (Principles 8, 10 and 11 of the Privacy Act)

- As a general rule, we should only use or share personal information in the ways we told people we would in our privacy statement (see below). These are our purposes for collecting the information.
- We can use or share personal information in new ways, as long we can satisfy one of the following exceptions:
    - It is directly related to the original purpose for which it was collected;
    - The person (or their representative) authorises us to use or share it in this way (remember, this should be a parent/guardian if a student is too young to provide meaningful consent);

  - It is necessary to prevent or lessen a serious threat to someone's life, health or safety;
  - It is necessary to assist a law enforcement agency to investigate an offence, or for the purpose of court proceedings (for example, custody proceedings);
  - The information is anonymised and will be used for statistical or research purposes.

- Where another law specifically requires or permits us to use or share personal information in a certain way, this overrides the Privacy Act. For example:
  - **Education Act** – requires us to share certain information with parents/guardians or the Ministry of Education.
  - **Oranga Tamariki Act** – requires us to share information about whether a child needs care or protection.
  - **Family Violence Act** – requires us to share information about family violence in certain circumstances.
  - **Police** – can require us to share specific information to assist with an investigation (but only with a search warrant).

- Information sharing for the purposes of student exchange schemes must comply with cross-border information sharing restrictions in the Privacy Act. All information sharing agreements must be approved by the Privacy Officer (Exec).

- We must also take care to ensure that we only disclose personal information when, and to the extent, that this is absolutely necessary to meet our purposes, and in ways that are appropriate and respectful. For example, we must be mindful of privacy when discussing a student's academic performance or wellbeing in the classroom setting or digitality.

Capturing and sharing images or footage

- There will be occasions where staff want, or need, to photograph or film classes, field trips, sporting events or other activities. This is acceptable, and images or footage may be used internally by Kristin for legitimate school purposes (such as reviewing team performance during a sporting event).

- However, before sharing images or footage publicly (whether online or in a newsletter or magazine), we must:
  - Confirm whether, at the time of enrolment, a student or their parent opted out of information sharing for publicity purposes.
  - Where the image or footage relates to students working in their own home (for example, when captured during a Zoom call), obtain explicit consent from the student or their parent to share it.
  - Consider whether there are any known safety concerns in relation to a student included in an image or footage.

- Where the image or footage includes people who are not associated with Kristin, such as students from other schools, confirm whether Kristin received a request not to publicise or broadcast images or footage about those people.
- Consider the content of the image or footage, to ensure that publicising or broadcasting it will not cause harm to the people involved. Further guidance on broadcasting footage of sporting events is available in the NZ Sport Collective's Charter on the Broadcast and Sponsorship of Secondary School Sport.

Managing privacy breaches

- A privacy breach means unauthorised or accidental access to, or disclosure, alteration, loss or destruction of personal information. Privacy breaches can be caused by internal factors (like employee browsing or poor security settings built into a system) or external factors (like criminal attacks on a system).
- Privacy breaches must be managed in compliance with the Kristin privacy breach management process:
  1. **Report** – Any person who becomes aware of a privacy breach must **immediately** report the breach to their Principal or Director and Privacy Officer (Ops).
  2. **Contain** – The Privacy Officer (Ops) must **promptly** determine what steps, if any, are required to contain the privacy breach and mitigate harm. This may require assistance from ICT staff.
  3. **Evaluate** – The Privacy Officer (Ops) must **promptly** determine the scope of the privacy breach, including the types of people affected and sensitivity of the personal information, and evaluate the likelihood of harm. Where a breach is serious, the Privacy Officer (Ops) must inform the Privacy Officer (Exec) and the Board of Governance.
  4. **Notify** – The Privacy Officer (Exec) must determine, in consultation with the Board of Governance, whether the privacy breach is a notifiable privacy breach and, if so, whether the Privacy Commissioner and/or affected people should be notified. A notifiable privacy breach must be notified **as soon as reasonably practicable** after Kristin has become aware of it.
  5. **Prevent** – The Privacy Officer (Ops) must investigate the cause of the privacy breach and determine what steps should be taken to prevent a recurrence.

Consequences of breaching this policy

Kristin emphasises the need to comply with the requirements of this policy. Any staff member, volunteer or contractor found to be in breach of the requirements of this policy may be subject to disciplinary action.

Kristin Privacy Statement

Our motto – **progress with vision, integrity and love** – drives the way we manage privacy and the personal information entrusted to us by our community – our students, alumni, parents, guardians and visitors. We keep it safe and use it only for good.

We see privacy as an integral part of our values-led approach to education. We need to collect and use personal information to do our jobs. Without this information, we cannot educate and grow our students, keep people safe or innovate. But we also know that maintaining the trust and confidence of our community is paramount.

What is this privacy statement?

This privacy statement explains what personal information Kristin collects, why we need it, how we use it, and who we share it with. It also explains how our community members can request or correct their information. In summary:

- We collect only the personal information we really need to meet our purposes, and as required by the Education Act.
- We take reasonable steps to protect the personal information we hold from harm.
- We use personal information in the ways set out in this statement, and only ever to meet our lawful school purposes.
- We only share information with others when we really need to, and we may have to share without consent if we think a community member is at risk.
- Community members have the right to request a copy of the personal information we hold about them, or to correct their information.
- Parents and guardians can generally request personal information about their children, but we must always put our students' best interests first.

We may update this privacy statement from time to time, for example to reflect changes to the Privacy Act, so take another look occasionally to see what might have changed. This statement was last updated in May 2020.

A note on consent

Where we are relying on consent, or authorisation, to collect, use or share personal information, we will generally seek this consent from a student's parent or guardian (as the student's representative).

However, there may be times where this is not appropriate, including where a student is over the age of 16 and the personal information in question is sensitive, or relates to matters over which the student may have a reasonable expectation of privacy.

What personal information does Kristin collect?

We collect personal information about our community members in several ways:

- We collect personal information **directly from the person** when they engage with us, for example completing an enrolment form or medical form.
- We collect personal information **from third parties**, for example from a student's family, from medical practitioners, or from other schools.
- We **generate** personal information as people use our services, for example when students engage in the classroom, meet with our health staff or move around the school campus.
- Several of our bus fleet are fitted with recording camera devices that record both image and sound – these are for health and safety purposes and to deter and follow up with any anti-sociable behaviour.

We collect a very broad range of personal information, and the information we collect about someone will depend on their role in our community – whether they're a student, alumni, parent or guardian, or a visitor to our school campus. The information we may collect includes:

- Personal details, including name, contact information, age, gender, and ethnicity
- Academic history
- Health information
- Information about academic performance
- Information about student behaviour and welfare, including family circumstances
- Attendance records
- Information about family/whānau and emergency contacts
- Photographs, audio, video or other media (for example during school trips or activities)
- CCTV footage (Kristin uses CCTV cameras on school premises for safety and security purposes, but not in private areas such as toilets or changing rooms)
- Information about use of Kristin digital resources and web portals, collected using log files or cookies

How does Kristin use personal information?

Our primary purpose for collecting personal information is to deliver educational services. To do this, we need to use personal information in the ways set out below. Where we need to use information in a way we have not anticipated here, we will only do so if required or permitted by law or with consent.

We use personal information to:

- Provide educational services to our students;
- Look after student educational, social and medical wellbeing and safety;
- Communicate with a students' parents, guardians or whānau about their education and wellbeing;
- Ensure the safety of our staff, volunteers, contractors, and visitors to our school campus;
- Manage and administer our school;
- Conduct marketing and communications activities (for Kristin, not third parties), manage events, and seek donations;
- Meet the requirements of the Education Act and other legislation, including reporting requirements; and
- For any other purposes that would be reasonably expected and are permitted by law.

We will only use sensitive information, like health information or information about suspected risks to a student's safety, for the purpose of ensuring that student's wellbeing. We will only use this information in other ways with consent or where permitted or required by law.

When does Kristin share personal information?

We need to share personal information in order to meet the purposes set out above. In all cases, we share with care and only ever disclose the minimum amount of personal information required to meet our purposes.

Sharing as part of the education system

We need to share general information about our students and community members in order to deliver educational services. This might include information about academic performance, reports, information about student behaviour, information required for planning school trips or events, or statistical information for reporting purposes.

We may share this information with:

- Parents, guardians, or whānau;
- Volunteers;
- Other schools (including overseas schools for student exchanges);

- Ministry of Education; or
- External Providers.

Sharing to keep students safe and well

Information about student health and wellbeing is generally only accessed by our health and counselling staff, who are subject to additional medical ethics requirements. However, sometimes, we may need to share sensitive information about our students or community members in order to keep people safe. This might include health information, information about student wellbeing, information about bullying, or any concerns we have about a students' family circumstances (including perceived risks of family violence).

This is always a difficult decision for us to make, as we may need to share personal information at these times against the wishes of a student. We always approach these decisions with care, and in the best interests of the student concerned.

We may share this information with:

- Parents, guardians, or whānau;
- Health agencies;
- Police;
- Oranga Tamariki; or
- Other government agencies.

Sharing to promote our school

We're proud of our school and our school community. This means that we want to share our achievements and the achievements of our students, to promote Kristin, grow our enrolment and raise the funds we need to deliver an exceptional educational experience.

For these purposes, we might share student work, student profiles, alumni profiles and career stories, or photographs and video footage of student trips or activities. At the time of enrolment, we provide students and their parents with the ability to opt out of this type of information sharing if they are concerned about it. We also take care to ensure that we do not share information about any students about whom there are safety concerns.

We may share this information:

- On our website;
- On the social media sites we use;
- In promotional materials, such as advertisements, brochures and prospectuses; and
- In our community publications, including our e-newsletter and Kaleidoscope Magazine.

How does Kristin store and protect personal information?

We store personal information electronically (on secure systems or platforms, including cloud platforms) or in hardcopy (in a secure physical location, including lockable cabinets). We may use third-party service providers to store and process personal information for us, some of which may store or process information overseas.

We retain personal information only for as long as we have a lawful purpose to use it, and we securely destroy or de-identify the information we no longer need. We follow Ministry of Education records retention and disposal guidelines, and generally retain personal information about a student for no more than 7 years after their enrolment with Kristin has ended, though we may retain some information (like name and contact information) for longer if we have a lawful purpose to use it (e.g. alumni networks) or in the public domain (e.g. school publications and awards).

We take all reasonable steps to protect personal information from loss, misuse, or unauthorised access or disclosure, including ensuring that only authorised staff or volunteers can access electronic platforms or physical storage, and that they access only the personal information they need to perform their functions. We won't ask you to use any third-party software or applications to interact with us unless we've assessed them first.

How do community members access or correct their information?

All community members – students, alumni, parents or guardians, or visitors – have the right to request a copy of the personal information we hold about them, or to ask us to correct it if they think it's wrong. Please direct requests to Kristin's Privacy Officer by:

- Emailing – kristin@kristin.school.nz;
- Calling – + 64 9 415 9566; or
- Writing to – Privacy Officer, Kristin School, PO Box 300087, Albany, Auckland 0752

We will process a request as soon as possible, and no later than 20 working days after we receive it. We will be as open as we can with the requester, and will only withhold information if we have a lawful basis. For example, we might withhold information if we believe that releasing it might involve the unwarranted disclosure of the affairs of another person, or might increase the risk of harassment or harm to another person.

Parents or guardians can generally request a copy of personal information about their child, on the basis that they are acting as their child's representative. However, we will always act in the best interests of our students, and if we believe releasing student information to a parent or guardian may not be in the student's best interests, we may refuse.

If we refuse to correct information because we believe it is accurate, the requester has the right to attach a statement to the information that explains the correction.

How do community members raise privacy concerns?

If you have any concerns about the way Kristin has managed your personal information, or information about your child, including the way we have responded to a privacy request, or if you wish to opt out of our promotional information sharing, please let us know. We will investigate your enquiry or complaint and will notify our decision as soon as practicable after it has been made.

Please direct privacy enquiries or complaints to Kristin's Privacy Officer by:

- Emailing – kristin@kristin.school.nz;
- Calling – + 64 9 415 9566; or
- Writing to – Privacy Officer, Kristin School, PO Box 300087, Albany, Auckland 0752

If we cannot resolve your concerns, then you have the right to complain to the Office of the Privacy Commissioner. Details for making a complaint to the Privacy Commissioner can be found at **privacy.org.nz/your-rights/making-a-complaint/**.

Student Privacy Statement

What's a privacy statement?

We're required by law to tell you things about the personal information we collect about you and how we use it. It's a good idea to read this, so you don't get any surprises later when you find out that we told someone else something about you.

What's personal information?

Personal information is any information that could be used to identify you or that is about you. It includes your name, email address or phone number. It could also include a picture of you or information about your studies. Personal information can be pretty sensitive too, like information about your health or when you tell us how something made you feel.

What info does Kristin need about me?

We need to collect all sorts of information about you to help you get through your education and stay safe and well. We collect most of it from you directly, and some from other people.

The sorts of information we might collect about you includes:

- **basic facts about you**, like your name, contact details, age, gender (like male, female or gender diverse) and ethnicity (like Māori, NZ European or Chinese)
- **information about your studies**, like your academic history, attendance, class reports, grades, and essays
- **Information about your health**, like disabilities, medical conditions, and your allergies or medications
- **Information about your welfare**, like the things you tell us about your family, conversations with our counsellors, or our observations from dealing with you
- **Photos or videos of you**, like when you go on school trips, or take part in events or classroom activities
- **Information about your use of Kristin digital resources**, like the school network or devices

What will Kristin do with my info?

We know that you care what we do with your information, and who we talk to about you. You can trust us to look after your information – we always have you best interests at heart – but we do need to use and share it to do our job.

- We share **information about your studies** with your parents or guardians, our volunteers, other schools, or the government when they ask.
- We might need to share more sensitive **information about your health or welfare** if we think you need help, including with your parents or guardians, your whānau, or the government if we think they can help.
- We might share **your successes** with our community. This might include using your photo on our website or sharing your work in our magazine. If you don't want us to do this, let us know.

We will usually ask your parents or guardians for consent to use or share your information, so have a chat with them about this, so they know how you feel about privacy.

Information about your health and wellbeing is generally only accessed by our health and counselling staff, who are subject to additional medical ethics requirements. If we need to talk to someone else about you when we think you might be unsafe, we will usually tell you first. We will share only the information we really need to help you. If you're worried about us talking to certain people about you, let us know and we can discuss this.

We will keep most of your information for no more than 7 years after your enrolment with Kristin has ended, though we may keep some information for longer if we need to.

How can I find out what info Kristin holds about me?

You, or your parent or guardian, can ask us for a copy of your information at any time, and you can ask us to correct your information if you think it's wrong. If you want to make a request, find out more about what we do with your information, or complain about something we've done, talk to your class teacher or Dean.

How can I protect my info and info about my friends?

Take a minute to think about the way you share your own information, or information about your friends. When you use apps on your phone, or share posts with friends on social media, remember that you're handing over a lot of information to these companies and to the world. This information doesn't go away, and you might feel differently about it being out there when you're older.

Remember to keep your devices password protected (and keep your passwords secret), be kind online (don't do or say anything you wouldn't do or say in real life), and don't share photos or videos of your friends without their consent.