PRIVACY
tauākī matatapu

Document Control			
Policy Manager:	Quality & Academic Unit Director	**Date First Approved:**	March 1996
Policy Owner:	Executive Director – Products and Planning	**Authorised by:**	Chief Executive
Category:	Operational	**Date Last Revised:**	May 2021
Wintec Taxonomy:	Information & Systems Management	**Next Review Date:**	April 2022

1. Purpose & Scope

This policy provides clarity to staff members and students regarding the collection, use, storage, and disposal of personal information. It also covers how to make a complaint, and how Wintec will respond. It explains our duties to you, your rights, and responsibilities.

We all have an obligation to take privacy seriously. We collect and store personal information on both staff members and students and have an obligation to protect that information. Staff members have the added responsibility of ensuring we collect, use, and dispose of personal information correctly.

Personal information is any piece of information that relates to a living, identifiable human being. This includes people's names, contact details, financial information, communication exchanges, and records of achievement. A person does not have to be named for the information to be identifiable.

This policy applies to all Wintec staff members, contractors, agents, and students.

2. Policy Statement

We are committed to managing personal information appropriately and within the limits of the law. We respect people's privacy while being clear about how we use, store, share and dispose of their information.

We manage personal information in accordance with the provisions of the Privacy Act 2020 (referred to as 'the Act') and Information Privacy Principles (IPP), the Health Information Privacy Code 2020, the Education and Training Act 2020, Public Records Act 2005 and the Official Information Act 1982. We are committed to:

2.1. Collecting only what we need

Whether you study at Wintec or work with or for us, we will only ask you to disclose the information we need to perform our duties for you.

2.2. Collecting information directly from you wherever possible

You will know what information we collect about you because we will ask you directly. Where we need to get information about you from another source, we will ask for your permission first.

2.3. Storing your information securely

We have clear policies and guidelines in place for our staff members to follow, and we take reasonable steps to store personal information securely. This includes (but is not limited to) using secure physical storage and electronic systems and making sure only appropriate people at Wintec have access to your personal information.

2.4. Upholding your rights

Including your right not to share information with us, your right to access information we hold about you, and your right to request correction of any information we hold about you.

In the unlikely event that we make a mistake, we will inform you, and the Office of the Privacy Commissioner, in accordance with legislative requirements.

2.5. Using, disclosing, and disposing of your information correctly

We will only use your information for the purpose for which we have collected it. We will only disclose it when we have your permission to do so, or when the law requires us to. We will dispose of your personal information securely and in line with relevant legislation.

This policy can be read in conjunction with Wintec's policies on:

- Information & Communications Technology Security
- Information & Records Management
- Social Media
- Media

This policy is not exhaustive. Several guidelines are available or in development for staff members on topics such as talent consent, and live streaming. Refer to *Section 8. Related Legislation, Regulations, Policies, Guidelines and Forms* of this policy for more information. Staff can also refer to the Privacy page on the Digital Workplace. Students and members of the public can refer to Wintec's Privacy page on the public website. If you have questions regarding this policy, or anything privacy related, please email privacy@wintec.ac.nz.

3. Key Roles & Expectations

This policy is owned by Wintec's Privacy Officer and managed by the Quality and Academic Director. The following roles have key responsibilities:

Students

- Treat any personal information disclosed by your fellow students, Wintec staff members and visitors with a high degree of privacy and respect
- report any privacy concerns, suspected, or actual breaches of privacy to any Wintec staff member, by emailing privacy@wintec.ac.nz, by writing directly to Wintec's Privacy Officer, or by contacting the Office of the Privacy Commissioner
- know your rights and responsibilities regarding personal information and know where you can seek help or advice in relation to this policy.

All Staff

- Adhere to this policy and are aware of the requirements for requesting, using, storing and correcting personal information; declining requests for personal information; obtaining consent to share/use personal information; raising concerns and/or complaints related to the use, disposal or sharing of personal information
- treat any personal information disclosed by fellow staff members, students, or stakeholders with a high degree of privacy and respect
- handle personal information requests appropriately in line with this policy and related procedures
- encourage secure, respectful practices regarding personal information
- complete any applicable privacy training and/or e-learning offered by Wintec

	• report any privacy concerns, suspected or actual breaches to your manager, via privacy@wintec.ac.nz, or directly to the Privacy Officer • know your rights and responsibilities regarding personal information and know where you can seek help or advice in relation to this policy.
Managers	• Work with your team members to ensure robust privacy practices are in place and that they are adhered to • support your team members in dealing with personal information requests, complaints, and other related matters as required, and escalate issues where appropriate • ensure that potential and actual privacy breaches and other privacy issues are identified and managed in accordance with this policy and with guidance from the policy manager and policy owner (the Privacy Officer).
Project Managers	• Must consider the role privacy and personal information plays in any new project or change of existing processes or systems that involves the collection, use or disclosure of personal information or that may impact the security or integrity of personal information held by Wintec • where applicable, complete a Privacy Impact Assessment (PIA) in accordance with this policy.
Quality Specialist	• Responds to enquiries from students, staff members and stakeholders regarding privacy matters • supports all staff members to understand and comply with the Wintec Privacy policy, including the development of relevant procedures, standards, and guidelines • reviews and investigates compliance matters related to privacy and reporting at Wintec • maintains the Register of Privacy Breaches and the Privacy Breach Management Plan on behalf of the Privacy Officer • assists with the management of privacy issues, including breaches and potential breaches • maintains the privacy email and Privacy page on the Digital Workplace and ensures resources, education and other content are maintained • aids the Privacy Officer as required.
Quality Assurance Unit	• Responsible for managing the review and implementation of this policy.
Privacy Officer	• Ensures that Wintec meets its statutory and accountability obligations concerning this policy and applicable legislation • conducts an annual assessment of this policy, its objectives and progress made toward achieving them • ensures the privacy breach management plan and register of breaches are maintained

	• conducts investigations into any suspected or actual breaches of privacy • manages privacy complaints received by Wintec and liaises with the Office of the Privacy Commissioner • currently the Executive Director – Products & Planning.
Executive Director – Communications & Events	• May conduct investigations into any suspected or actual breaches of privacy on behalf of the Privacy Officer.
Privacy Breach Management Team	• The Privacy Officer has the choice to convene the Privacy Breach Management Team (PBMT) in the event of suspected or actual privacy breach where serious harm has or could occur • the PBMT consists of the Privacy Officer; Executive Director – Communications & Events; Director – Quality & Academic Unit (or representative), Contracts Office Manager (or representative), and the Information & Records Manager • depending on the circumstances of the breach, the PBMT will also include other Executive Directors and/or senior managers.
Chief Executive	• Approves this policy • monitors objectives, issues, complaints, resolutions, and any other applicable developments as required.
Wintec Board	• Ensures Wintec meets its statutory and accountability obligations • responsible for oversight of the effectiveness of this policy.

4. Measuring Success

The measurements of successful management of privacy at Wintec are:

- We request, use, store and dispose of personal information in line with the Privacy Act 2020, Information Privacy Principles, the Health Information Privacy Rules, and the Public Records Act 2005.
- We do not breach the privacy of any of our students or staff members nor receive complaints due to our actions or inaction regarding privacy.
- All requests for personal information are managed in accordance with this policy and within the limits of the Privacy Act 2020 and Official Information Act 1982.
- Personal information is used only for appropriate business purposes.

5. Important Information

Wintec staff members and contractors can visit the Privacy page of the Digital Workplace for more information on managing privacy. Students can visit the Privacy page of our public website. Questions regarding these topics can be addressed to privacy@wintec.ac.nz or to the Privacy Officer.

5.1. Collection of personal information

Wintec collects a lot of information from many sources over the course of providing our services to students and the wider community. Staff members must only collect what they need for a lawful purpose (one related to Wintec's functions or activities). This encompasses all systems, processes, forms, and procedures.

Careful consideration must be given to the purpose for collection – if the information is not necessary to conduct Wintec's activities then it should not be collected. Refer to IPP 1 (purpose) and 4 (manner of collection) of the Act.

Consideration must be given to whether it is fair and legal to collect the personal information. It should be collected from the person directly whenever possible, unless it can be reliably collected from a third-party authorised by the person, or via another government agency. Refer to IPP 2 (source).

When we collect personal information from a person, we must ensure they are aware of the following:

- what information is being collected
- why we are collecting the information
- how we will use the information
- with whom the information will be shared
- whether the information requested is compulsory or voluntary
- what will happen if the information is not provided
- how long we will keep this information for, and
- the person's rights regarding the access and correction of that information.

When the information collected is routine and at organisational level, such as during enrolment, it is sufficient for the privacy statement viewed and accepted by the person at that time to cover these routine activities (provided the privacy statement meets the awareness criteria above). Routine activities include organisational wide activities considered a normal part of Wintec's processes.

If the information collected is at School/Centre/Business Unit, programme or module level (for example, work placements, criminal history checks, noho marae visits, field trips) or could be considered unusual or ad hoc (such as may be required during a pandemic response, or for a research project) then a specific privacy statement may be required relating to that collection.

Staff members should consult the Privacy page for assistance crafting a suitable privacy statement.

5.2. Use and disclosure

It is important to understand when personal information can be disclosed to another party, and the checks that must be undertaken before doing so. Staff members must take reasonable steps to ensure that personal information is accurate and up to date before using or disclosing it, as per IPP 8 (accuracy). This is particularly important where this use or disclosure could affect the rights or interests of the person.

Personal information collected by Wintec staff members should only be disclosed by those staff members if that use or disclosure is for the purpose for which it was collected in the first place, and that this disclosure was made clear by the relevant privacy statement used at the time it was collected. In addition, IPP 13 (unique identifiers) governs the use of personal information linked to unique identifiers such as Wintec Student ID numbers.

Staff members who want to use or disclose information in ways not covered by the original privacy statement must seek permission from the person. If this is not possible, staff members must be able to rely on an exception covered by Information Privacy IPP 10 (use) or IPP 11 (disclosure). If unsure,

you consult the Privacy Officer or email privacy@wintec.ac.nz before sharing or disclosing the personal information.

Wintec is responsible for ensuring that any contracted third-party service provider, individual, agency or organisation either in New Zealand or overseas with whom we share a person's information is either a) subject to our privacy laws b) subject to similar privacy laws with comparable safeguards, subject to the disclosure criteria in IPP 11 (disclosure) or IPP 12 (disclosure outside New Zealand). They must be able to provide a suitable level of protection for any personal information shared.

In situations where disclosure is necessary to avoid immediately endangering a person's health or safety, or when disclosure is required to enforce or uphold the law, staff members may disclose certain personal information about a person. Staff members can also use and disclose information provided it does not identify the person concerned (e.g. statistical information).

Refer to Section 6.3 *Disclosing Personal Information*, for more information on the steps involved.

5.3. Storage, security, and retention

All Wintec staff members have a responsibility to protect the personal information we collect and use against loss, theft, misuse, unauthorised access or disclosure; see Principle 5 (storage and security). Wintec stores some of the personal information we collect on servers located in other countries (such as Australia). This means that the personal information we hold may be transferred to, or accessed from, countries other than New Zealand. We ensure that our third-party data processors meet our privacy and security requirements, and those of the Act.

Staff members are expected to use Wintec approved technologies. Staff members are only permitted to use Wintec approved services and applications to store personal information about students or staff; they are not to transfer that personal information onto USB or other non-Wintec approved external hard drives or storage devices under any circumstances.

When staff members collect information in physical form such as enrolment applications or forms that require a physical signature, these must be kept physically secure and in spaces not accessible by the general public or non-Wintec approved staff members.

We take all reasonable steps to ensure the personal information we collect is protected against loss, unauthorised access and disclosure or any other misuse, including meeting the requirements prescribed by Te Rua Mahara O Te Kawanatanga – Archives New Zealand, for the storage and disposal of personal information. We retain information only so long as it is administratively required, in compliance with the requirements of the Public Records Act 2005, and IPP 9 (retention). Personal information must be disposed of in accordance with Wintec's General Disposal Authority. For more information, staff members can refer to our Information & Records Management policy or the Privacy page on the Digital Workplace.

IT and communications security are vital components of personal information management. All staff members must read and understand our Information & Communication Technology Security policy, and be familiar with our Mobile Technology and Technology Use policies. New staff members and contractors sign a Protection of Privacy and Confidentiality agreement upon beginning their employment at Wintec.

Staff members must only access or use personal information when necessary for legitimate purposes. Employee browsing – using ICT systems to unnecessarily access personal information of students or staff members – is strictly prohibited, and cases of this could result in disciplinary action being taken.

5.4. Access and correction

Every person we collect data from or about, has the right to access the information we hold about them, in accordance with IPP 6 (access). This right extends to their authorised representative if they

have one. People can also request the correction of information held about them by Wintec – see IPP 7 (correction) – and must be advised of this right when personal information is released to them. These are known as Personal Information Requests (PIRs). A person can make this request via email, letter, phone or in person. The staff member who receives this request must ensure they keep a record of this request.

Staff members are expected to provide information promptly. However, if staff members are concerned about the release of information for practical, safety or other reasons, they should email privacy@wintec.ac.nz or contact the Privacy Officer to discuss. In most situations, Wintec must respond to personal information requests within 20 working days. There are specific reasons personal information can be withheld. These can be found under Part 4 of the Act. If a staff member refuses to release information, a written explanation must be provided to the person requesting.

If a person believes the information Wintec has about them in wrong, they can request it be corrected; referred to as a Statement of Correction. Staff members who receive a request are expected to correct this information. If there is reason to believe it does not need correcting, the staff member may refuse the request. In this case, the staff member must email privacy@wintec.ac.nz first.

If the PIR is declined, Wintec will attach or record the Statement of Correction to the personal information, along with our written decision. Wintec must ensure that personal information held is accurate, complete, relevant and not misleading; Principle 8 (accuracy).

For more on PIRs, refer to Sections 5.9 and 6.1 *Personal Information Requests*, in this policy. For more on the steps involved in correcting information, refer to Section 6.2 *Correcting Personal Information*, in this policy.

5.5. Reporting a privacy breach

A privacy breach is defined as any unauthorised access, disclosure, alteration, loss, or destruction of personal information. It can also be any action that prevents access to personal information (either temporarily or permanently).

Breaches in privacy could cause harm to students, staff members, our stakeholders and wider community. If managed poorly, a privacy breach could cause significant damage to Wintec's reputation and the wider tertiary education sector. We must act quickly to manage any situation that arises, and ensure the right people are involved at the right time.

Staff members must report potential, suspected or actual privacy breaches promptly to their immediate manager, via email to privacy@wintec.ac.nz, or directly to the Privacy Officer, in compliance with Wintec's Privacy Breach Management Plan. Actual breaches or near misses are also recorded in the Register of Privacy Breaches, maintained by the Quality and Academic Unit.

Where the breach is also an ICT security issue, it must also be reported to the Information Technology Services (ITS) team by logging a case (either email servicedesk@wintec.ac.nz or phone 0800 494 6832). For more information, refer to the Information & Communication Technology Security policy.

Students must ensure in the event they become aware of a suspected or actual privacy breach, that this is reported promptly. Students can report this to their tutor, programme manager, via privacy@wintec.ac.nz or directly to Wintec's Privacy Officer.

All Wintec staff members and students should report suspected or actual privacy breaches. Our privacy efforts are focused on education, transparency, and accountability; everyone should feel safe to raise privacy issues. Once identified, we can take steps to address and manage any issues or breaches, in accordance with Wintec's Privacy Breach Management Plan.

When there is a likelihood that a privacy breach could cause serious harm, Wintec is required to notify the Privacy Commissioner and, in most cases, the person(s) affected. This is called a notifiable privacy breach. These notifications are managed by the Privacy Officer.

The relevant factors considered when determining if serious harm has or could occur include the:

- sensitivity of the information
- actions taken to reduce harm
- nature of the harm
- people or organisations who have the information
- accessibility and security of the information
- existence of other relevant matters

Any person also has the right to notify the Privacy Commissioner directly of a breach in privacy. For more information refer to Section 6.4 *Managing a Privacy Breach*, in this policy.

5.6. Cultural considerations and privacy

Different cultures have different approaches to privacy. In most cases, New Zealand's privacy laws are flexible enough to meet the needs of different cultural interpretations of personal information and privacy. Wintec supports *mana motuhake*, the right to Maaori self-determination and sovereignty over a person's personal information and data. To avoid any confusion, the intent of mana motuhake and Wintec's Privacy policy apply to all people's, irrespective of culture or ethnicity. Whaanau/family have several options available for requesting information on rangatahi/young people studying at Wintec. See Section 5.9 *Personal Information Requests* or Section 9. *Key Definitions* for more information.

5.7. Privacy Impact Assessments

Project Managers are expected to incorporate privacy matters into the design and development of new or changing systems and processes, to ensure that the rights of users are maintained, and that personal information is only collected when necessary. Completing a Privacy Impact Assessment helps when considering the impact of functionality, security, visibility and transparency on personal information. Respect for the user's privacy is the core principle of this approach.

For more information, refer to Section 6.5 *Conducting a Privacy Impact Assessment* in this policy, or email privacy@wintec.ac.nz.

5.8. Making a complaint

If you feel your privacy has been breached, you are entitled to make a complaint to Wintec. Any staff member, student or member of Wintec's community can make a complaint or address their questions or concerns by contacting Wintec's Privacy Officer via email privacy@wintec.ac.nz or by writing to this address:

Privacy Officer
C/o- Quality & Academic Unit
Wintec
Private Bag 3036
Waikato Mail Centre
Hamilton 3240

Note that the Privacy Officer may engage with or escalate a complaint to other departments and/or staff as part of any investigation into a suspected or actual privacy breach.

Staff members and contractors can also refer to the Employee Complaint Management policy for more information on the process Wintec follows for complaints.

Students can refer to the Student Voice policy for how Wintec manages complaints from students.

The Privacy Commissioner can be reached via their website.

5.9. Personal Information Requests

It is generally accepted that Wintec will release to a person the personal information we hold about them, upon their request. Personal Information Requests (PIR's) can be made in person, via email, a letter, or over the phone. A person does not have to refer to legislation to make a request.

In most cases, personal information requests are likely to cover small amounts of personal information, and Wintec staff members can disclose the information in as reasonably a practicable time as possible, provided they have ascertained the identity of the person making the request, and their legitimacy to make the request.

Under the Privacy Act 2020, once the request has been received, Wintec has 20 working days to respond. If the request is urgent, we have a responsibility to respond as soon as practicable. Depending on the nature of the request, we may have to clarify with the person what information they are requesting, and may request, within reason, more time to comply with the request (if it is complex or sensitive in nature).

Wintec can choose to withhold information in some cases, for example where releasing the information would breach the privacy of another party, breach legal privilege, is frivolous or vexatious in nature, or the release may cause unnecessary or serious harm to the person or others; but personal information should only be withheld where absolutely necessary. When staff members receive a request for information that may be complex, relates to a substantial amount of information, is sensitive in nature (such as an employment issue or student complaint) or they believe the request may otherwise meet one of the criteria above, then the Privacy Officer must always be consulted before the request is actioned. Contact the Privacy Officer directly, or email privacy@wintec.ac.nz.

There are requirements in the Privacy Act 2020 that Wintec must comply with when managing PIRs, including timeframes and when to release/withhold personal information. Breaching these rules can result in an automatic breach of the person's rights and may lead to a complaint and investigation by the Office of the Privacy Commissioner. The responsibility is Wintec's to be as open and transparent as possible with the person making the request. See Part 4 of the Act.

Wintec can release personal information to a person's authorised representative, provided we have the person's consent to do so. Staff members must ensure that they have the permission of the person concerned before releasing any personal information about them. Permission can be given in person, via email, a letter, over the phone or by the person completing an Authority to Act form (currently in development).

If a request is made by a person or agency for information about someone else, or information that is not personal information, then this is an Official Information Act request, and different procedures are followed. For more information, staff members should refer to our Media policy.

Refer to Section 6.1 *Personal Information Requests* and Section 6.3 *Disclosing Personal Information* for more on the steps involved.

6. Procedures

The following procedures apply to all Wintec staff members, contractors, and where applicable, students and members of the wider Wintec community. If any staff member, contractor or student has questions about these procedures they should email privacy@wintec.ac.nz.

6.1. Personal Information Requests

This procedure sets out the process for managing a Personal Information Request (PIR). It applies to all Wintec staff members and contractors who may receive and/or manage a PIR.

a) **Receiving the request**: A PIR can come in any form, including in person, via letter or email, or over the phone. A person making the request doesn't have to mention the Privacy Act 2020; if the information they're requesting is their own, they are entitled to request it.

b) **Verify the identity of the person making the request**: Personal information can only be released to the person to whom it belongs, or to the person they have authorised us to release it to. If the PIR is not made by the person, check we have written authority to release to their authorised person on file. If they are not entitled to the information, you must not release it. If the request is being made via email, check they are using a recognised email address, and confirm their identity.

   Students who wish to nominate an authorised person to act on their behalf can complete an Authority to Act form (TBD), or provide information to us, as per the instructions on our public website.

   Note: If you believe the request for information is being made under duress, or the threat of physical or mental harm to or by the person making the request, or others, contact the Privacy Officer or email privacy@wintec.ac.nz as soon as possible to discuss.

c) **Record the time and date of the request**: A PIR must be responded to as soon as reasonably practicable, but no later than 20 working days from the day it was received. Personal information does not need to be released at the same time the request is received, though in practice usually is.

   A person is also entitled to make a request under urgency, provided they have a good reason for making the request (such as an immigration matter or for legal proceedings). If the PIR is deemed urgent then it must be responded to as soon as reasonably practicable. Failure to do so could result in Wintec breaching the person's rights.

d) **Confirm the complexity of the request**: Is the PIR straightforward?

   I. If yes, you should release the information as soon as practicable. Record the date and time the information has been released, and if applicable, include the PIR in the appropriate location relating to the information being released. End of procedure.

   II. If the PIR is urgent, or involves sensitive information (such as an employment dispute, student complaint, or any personal health information) or the request is for complex information (such as all the information Wintec has on the person) that will take time to respond to, then proceed to the next step.

   Note: Make sure you understand what is being requested. You can ask for clarification on the information being requested from the person.

e) **Escalate the request**: Having established that the PIR is not straightforward, you must escalate this. Discuss any urgent, sensitive or complex PIR with your manager in the first instance.

If it cannot be resolved, you must email privacy@wintec.ac.nz, or contact the Privacy Officer. You will be advised how to respond to the request.

For complex or sensitive requests, Wintec may need more time to process the request. If this is the case, the Privacy Officer will write to the person advising them the reason(s) why.

f) **Locate the information**: A complete search of all relevant systems must be undertaken, including desktops and email account of relevant staff members, particularly when a person has requested all the personal information Wintec holds on them.

Note: If Wintec does not hold the information requested but knows who does, the Privacy Officer will advise the person. If the other party is a New Zealand government agency, we must transfer the request to that agency within 10 working days of being received.

g) **Decide what to release**: While Wintec will generally release all personal information to the person requesting, the following must be checked first:

- Accuracy: Is the information accurate to the best of your knowledge?
- Completeness: Is the information gathered a complete record of the personal information requested?
- Identity: Has the identity of the person making the request being confirmed? Are they legally allowed the information?

Note: If the answer to any of these questions is 'no', then you cannot release the information. Email privacy@wintec.ac.nz to discuss.

- Rights of others: In releasing the personal information to the person, would this infringe upon the privacy rights of others?

Note: We must ensure that in releasing information we are not breaching the privacy rights of another person.

In some instances, it may be necessary to withhold personal information or refuse a PIR. Information may only be withheld in accordance with Part 4 of the Act, specifically section 46 and sections 49 to 53. Any decision to withhold personal information under these grounds must be approved by the Privacy Officer.

Note: A person has the right to request all their information. A PIR cannot be refused on the basis that the person is unable or unwilling to minimise the amount of information requested.

h) **Contact the person**: Once a decision has been made regarding the PIR, you must advise the person who made the request as soon as possible, and within the 10 or 20 working days, as applicable. Your response must outline what information will be released, and what, if any, is being withheld. Grounds for refusal to disclose must be advised, in accordance with the Act.

i) **Release the information**: If the information has not already been released, then it must be released as soon as it practicably can be. If there has been or is likely to be a delay in releasing the information, this needs to be explained to the person in writing.

j) **Record the release of information**: Including the date and time the information has been released, the PIR and a copy of the decision or release letter must be in the appropriate location relating to the information being released. End of procedure.

6.2. Correcting Personal Information

This procedure sets out the process for managing a request to correct personal information. It applies to all Wintec staff members and contractors who may receive and/or manage such a request.

a) **Receiving the request**: A request to correct personal information held by Wintec can come in any form, including in person, via letter or email, or over the phone. A person making the request doesn't have to mention the legislation; as long as the information they're requesting is their own, they are entitled to request it be corrected.

b) **Determine whether to correct**: A person's right to correct personal information held about them is not absolute under the Act. Where a person's details are clearly wrong (such as the wrong contact details) then it is appropriate to fix. However, when a person is seeking to change an opinion (such as one might expect to find in documentation about a complaint) then Wintec is not obligated to correct this information.

c) **Statement of Correction**: If correction is not appropriate, then the request must be attached to the disputed information, along with an explanation. This is called a Statement of Correction.

d) **Advise the outcome**: Whether personal information has been corrected or not, the person who made the request must be advised of the outcome, either verbally, in person, over the phone, etc. (for minor changes), or in writing if a Statement of Correction has been issued.

e) **Informing other people or agencies**: Where applicable, if we have passed incorrect information about a person on to another person or agency, we are required to inform them that the information has been corrected. End of procedure.

6.3. Disclosing Personal Information

This applies to all Wintec staff members and contractors who may be required to disclose personal information or respond to third-party requests for personal information, who manage projects or systems that impact on personal information, or who make decisions about the way Wintec manages or discloses personal information.

Before disclosing, advice should be sought to ensure that disclosure is directly related to the purpose of the original collection. Staff members and contractors who have questions about whether or not they can disclose personal information in a particular case should email privacy@wintec.ac.nz or discuss with the Privacy Officer directly.

a) **Purpose of the disclosure**: Personal information at Wintec can be disclosed when this was one of the purposes advised at the time the information was collected. Our Privacy Statements provide notice to people about the ways their personal information will be used and disclosed.

b) **Routine disclosure**: Personal information disclosed on a routine basis must be done securely in compliance with this and the Information & Communication Technology Security policies.

c) **Disclose only what is necessary**: Any staff member or contractor disclosing personal information must ensure that they disclose only what is necessary to the extent that it meets the relevant legitimate purpose or purposes.

d) **Disclosure for lawful purposes**: Wintec may need to disclose personal information in ways that have not always been addressed in Privacy Statements (such as in response to a request from a government agency) or where an information sharing agreement does not exist. These disclosures are acceptable, provided they are legitimate and have a lawful basis.

   In some instances, specific legislation or statutory powers may compel Wintec to disclose information. These must be in writing. Certain provisions override the Act. For example:

   - Section 22C of the Health Act 1956 requires our staff to disclose health information where they are requested to do so by certain public officials, including a Probation Officer, the New Zealand Transport Agency or a social worker.

- Section 11 of the Social Security Act 1964 gives the Ministry of Social Development power to obtain information for carrying out certain purposes.
- Section 17 of the Tax Administration Act 1994 gives the Inland Revenue Department requires that information to be furnished at the request of the Chief Executive of IRD.
- Section 74 of the Search and Surveillance Act 2012 gives law enforcement agencies such as the New Zealand Police the right to order a person or organisation to provide personal information as evidential material of a specified offense.
- Section 120 of the Coroners Act 2006 compels a person to release personal information to the Coroner when requested in writing. Refer to the Media policy for more information.

Note: Requests from the police or other law enforcement agencies must be escalated to the Privacy Officer as soon as practicable.

e) **Disclosure on health and safety grounds**: Where disclosure is deemed to be necessary to prevent or lesson a serious threat to public health, public safety, or the life or health of the individual concerned or another individual, then it can be disclosed.

Note: In this instance, the request to disclose should be escalated to the Privacy Officer prior to being actioned. If the Wintec staff member or contractor is unable to escalate to the Privacy Officer before releasing the information, they must advise the Privacy Officer as soon as practicable following the release.

f) **New purposes for use and disclosure**: Personal information can, in some cases, be disclosed for new purposes. In these instances, staff members and contractors must consider the following:

I. Can we disclose the information without revealing personal information? Such as by compiling statistical information or generalised data? Wintec can disclose information for research or statistical purposes provided it is in a form that could reasonably be expected not to identify the person(s) concerned.

II. Can we ask the person to authorise the disclosure? If the purpose is significantly different from the purpose for which it was originally collected, we may need to ask permission to use their personal information for this new purpose.

III. Is the source of the information from a publicly available publication, and it would not be unreasonable to disclose it?

IV. Can the request for disclosure be dealt with under the Official Information Act 1982? Requests for personal information made by a third-party such as a news or media agency may be dealt with by OIA requests. Refer to the Media policy for more information.

g) **Disclosing to a new contracted service provider**: Before disclosing information to a new contracted service provider, staff members and contractors must ensure that the service provider has comparable safeguards for protecting personal information.

This applies to both domestic and international service providers, agencies, and persons. For international agencies and individuals not present or resident in New Zealand, the Act has additional specific provisions for cross border data transfer, that must be adhered to; such as IPP 12 (disclosure outside of New Zealand).

Refer to Section 6.5 *Conducting a Privacy Impact Assessment* for more information on considerations that must be given when engaging a new contracted service provider.

Note: transferring of personal information to other agencies is not considered disclosure, provided they are not accessing or using the information for their own commercial or other

purposes. Under no circumstances are foreign or domestic third parties, agents, agencies individuals or commercial entities allowed to use personal information collected by Wintec or on Wintec's behalf without the express written permission of the Privacy Officer, or the permission of the person whose data is to be disclosed. End of procedure.

6.4. Managing a Privacy Breach

This procedure sets out the general process for what to do in a privacy breach. Where a serious or potentially serious breach has occurred, the breach will be managed in accordance with the Privacy Breach Management Plan. This applies to all staff members, students, and contractors.

a) **Report the breach**: the following options are available to report a privacy breach:

- Students can inform any Wintec staff member of a suspected or actual privacy breach.
- Any Wintec staff member or contractor who causes, witnesses or otherwise discovers an actual or suspected privacy breach (near miss) must as soon as practicable report the breach to their manager and/or the Privacy Officer, or email privacy@wintec.ac.nz.
- Where the breach is also an ICT security issue, it must also be reported to the Information Technology Services (ITS) team by logging a case either via email servicedesk@wintec.ac.nz or phone 0800 494 6832. For more information, refer to the Information & Communication Technology Security policy.
- Members of the community can report a suspected or actual privacy breach of Wintec related personal information by emailing privacy@wintec.ac.nz, by calling Wintec on 0800 294 6832, by writing to Wintec's Privacy Officer, or contacting the Office of the Privacy Commissioner.

b) **Assess the breach**: On being notified of the breach, the Privacy Officer must assess the scope and likelihood or risk of serious harm to the person(s) involved, and the risk to Wintec. Privacy Officer to consult with the relevant parties, as per the Privacy Breach Management Plan. Note that the Privacy Officer may engage with other departments and/or staff as part of any investigation into a suspected or actual privacy breach. For more information, refer to Section 5.5 *Reporting a Privacy Breach*, in this policy.

c) **Contain the breach**: Following the guidance of relevant parties the Privacy Officer to determine what steps are required to contain the breach and ensure that appropriate action is taken.

d) **Determine if the breach is notifiable**: The Privacy Officer will determine whether the breach has caused or is likely to cause serious harm and is therefore a notifiable privacy breach.

e) **Notify the Privacy Commissioner**: Where the Privacy Officer has determined that the privacy breach is notifiable, they must notify the Office of the Privacy Commissioner, and other relevant agencies if applicable, as soon as reasonably practicable.

f) **Notify the person(s) affected**: In most instances, the Privacy Officer must also notify the person(s) concerned. The Privacy Officer may, where appropriate, direct the relevant manager or another Wintec staff member to manage the notification of the data subjects affected. The Privacy Breach Management Plan contains the specific requirements of a notification.

There are exceptions under Section 116 of the Act, where immediately notifying the person(s) affected may not be appropriate. The Privacy Officer will determine whether an exception applies.

g) Update the Register: The Privacy Officer ensures the Register of Privacy Breaches is updated. Any follow up actions will be dealt with accordingly. End of procedure.

6.5. Conducting a Privacy Impact Assessment

This procedure applies to all staff members who manage projects or systems that collect, use or store personal information, or who make policy or procedural decisions about the way Wintec manages personal information.

Privacy Impact Assessments (PIAs) are required when changes present a high risk to the safety and security of personal information about students or staff members. By following this procedure, you ensure that Wintec is more likely to comply with the Privacy Act, while cementing privacy as a key consideration incorporated into the design stage of any project or process implementation.

a) **Understand the privacy implications**: Whether engaging a new contracted service provider, embarking on a new project, or redeveloping an existing process or system, consideration must be given to the following:

- Collection: Wintec must limit the amount of personal information collected and retained to only what is required to carry out its duties.
- Openness: Wintec must be honest and transparent about the information collected and how it will be used.
- Disclosure: Wintec must use personal information appropriately, and limit disclosure to only when necessary or legally required.
- Security: All reasonable and practicable steps must be taken to protect personal information collected.
- Rights: Users must be informed of their privacy rights, including the right maintain control of their personal information.

b) **Determine if a PIA is required**: Only those changes that present a high risk to personal information require a PIA. To determine, consider the following:

I. Does the change include any involvement or alteration of personal information? This includes the collection, storage, use or disclosure of such information. If not, then a PIA is not required. If yes, proceed to the next point.

II. Is the personal information sensitive in nature? Sensitive information includes any information where a person could reasonably expect a higher degree of protection, or where there is a likelihood of harm or serious harm, should their information be mishandled.

For example: student or staff member health information, research data (involving persons regardless of whether they are students or staff members), employee complaints, performance or remuneration details, or financial information (such as bank account details or pay slips). If not, then proceed to the next point. If yes, then a PIA is required.

III. Would the change put personal information at risk? For example, transferring a large amount of personal information from one service provider to another, or through the merger of existing databases or when upgrading systems. If not, then proceed to the next point. If yes, then a PIA is required.

IV. Could the change cause controversy or negatively impact reasonable expectations? For example, through the use of intrusive technology to track user movements or by transferring a large amount of personal information from one service provider to another, a merger of existing databases or upgrading to new systems. If not, then no PIA is required; process ends. If yes, then a PIA is required. Proceed to the next step.

c) **Conduct the PIA**:

I. For new projects or changes to existing systems or processes, Project Managers (or relevant staff) must complete the Privacy Impact Assessment Checklist (currently under development).

II. When engaging a new contracted service provider, consideration must also be given to:

- Location: If the service provider is not based in New Zealand, we either require the permission of the person(s) whose personal information we are managing, or the service provider must be conducting business in New Zealand, and be subject to privacy laws with comparable safeguards to the Privacy Act 2020, or participate in a prescribed Binding Scheme, subject to the laws of a Prescribed Country, or have comparable contractual safeguards.
- Limitations: The service provider must not be able to access, use or disclose personal information for its own purposes.
- Privacy Breaches: The service provider must agree to alert Wintec as soon as reasonably practicable of any breaches or potential breaches that impact the security of information stored by them on behalf of Wintec.
- Retention and Control: On termination of a relationship with a service provider, any personal information stored by a service provider must be returned to Wintec. Under no circumstances should the service provider retain any information gathered by or on behalf of Wintec.
- Compliance: The service provider must not hinder Wintec's ability to meet its obligations under the Privacy Act 2020.

Privacy is covered by contractual clauses in agreements between Wintec and third parties. Where staff members are dealing with privacy issues in the context of a contract, they should contact the Contracts Office in the first instance.

d) **Incorporate PIA results into the change**: Project Managers are to include privacy considerations as BAU. The completed PIA must be emailed to privacy@wintec.ac.nz.

7. Processes

There are no published process maps for this policy. Staff members and contractors should refer to the Privacy page on the Digital Workplace for more information. Students and members of the public can view the Privacy page of Wintec's public website for more information.

If any member of the Wintec community has questions about this policy or these procedures, they should email privacy@wintec.ac.nz.

PRIVACY
tauākī matatapu

8. Related Legislation, Policies, Guidelines, and Forms

Legislation/Regulations	Policies	Guidelines/Forms
Privacy Act 2020 Health Information Privacy Code 1994 Education and Training Act 2020 Public Records Act 2005 Official Information Act 1982	Information & Communications Technology Security Information & Records Management Social Media Media Mobile Technology Technology Use	Wintec privacy page on the digital workplace Privacy Breach Management Plan Privacy Impact Assessment Checklist (WIP) Authority to Act process and form (WIP)
Copies of relevant legislation can be found on the New Zealand Legislation Website. You can view Wintec's policies, procedures, and guidelines on the Digital Workplace. This is not an exhaustive list of policies, procedures, and legislation.		

9. Key Definitions & Glossary

Authority to Act — The process of giving a person authority to act on your behalf. Especially relevant to students, they can authorise their nominated person to have access to personal information held by Wintec about them. A nominated person can be anyone but is typically a whanau/family member. Unless Wintec has authorisation from the person or is otherwise acting on their behalf (such as an enduring power of attorney) we will not discuss with any person their family member's personal information.

Binding Scheme — Regulations, conventions or provisions that exist under different countries' legislative tools that contain similar clauses to New Zealand's privacy laws. The Office of the Privacy Commissioner has yet to provide further guidance on these, but similar binding schemes are likely to include those found in:

- The European Union's General Data Protection Regulations (GDPR) 2018;
- Australia's Privacy Act 1988, and
- California's Privacy Rights Act 2020.

Disclosure — The act of revealing personal information to any person, party, contracted service provider, agent or agency. Does not include sharing personal information between Wintec staff members either electronically or in person for the purposes of carrying out their duties. For personal information requests by the subject of the information, the person would make a PIR.

See also, *Personal Information Request*.

Employee Browsing — The practice of employees accessing personal information about other staff members or students inappropriately and without a legitimate reason to do so. It is any kind of browsing of information that serves no purpose towards the role, responsibilities and duty of care we have towards our students and staff members. It does not include searching personal information for legitimate purposes. Wintec is obligated to keep information safe and secure. This

	includes protecting it against unauthorised or inappropriate access by our staff members and contractors.
Health Information Privacy Rules	Similar to the Information Privacy Principles, the 12 Health Information Privacy Rules are found in the Health Information Privacy Code. The rules are similar to the privacy principles but are applied in a health context.
Information Privacy Principles	Also known as IPP, the principles 13 principles of the Privacy Act 2020 govern how we collect, handle and use personal information. See also, *Privacy Act 2020*.
Mana motuhake	In a privacy context, mana motuhake refers to the right of a person to have control of their personal information, and exercise self-determination and autonomy over one's own identity and personal information.
Notifiable Privacy Breach	A formal notification to the Office of the Privacy Commissioner and affected parties A privacy breach is notifiable if it is reasonable to believe that a privacy breach has caused, or is likely to cause, serious harm to an individual. See also, *Serious Harm*.
Personal Information	Personal information is any piece of information that relates to a living, identifiable human being. This includes people's names, contact details, financial information, communication exchanges, records of achievement: anything that identifies a person. A person does not have to be named for the information to be identifiable. In determining whether or not certain information could be considered personal, consideration must be given to whether there is a reasonable chance someone could be identified by the information. While information such as a name, phone number or address etc., is obviously personal, it can also include less obvious information such as biometric information and behavioural information. Some information, such as a bank account number, may not be identifiable on its own, but when combined with other data, can become identifiable personal information. This type of information is classified as a unique identifier, and the Privacy Act applies. Not all information we collect or hold comes under the definition of personal information: Business practices, policies, trade secrets, and email addresses are not considered personal information in the first instance, but rather administrative information. It is however, context specific, and in these instances, advice should be sought from the Privacy Officer or by emailing privacy@wintec.ac.nz.
Personal Information Request	Also known as a PIR. This is a request to either access, update or correct a person's information, by the person or their authorised representative or nominated person. A person can make this request via email, letter, phone or in person. The staff member who receives this request must ensure they keep a record of this request. The person does not have to quote any legislation when making such a request. See also, *Statement of Correction.*

PRIVACY
tauākī matatapu

Privacy Act 2020	New Zealand's privacy law as of 01 December 2020. It applies to all New Zealand and overseas agencies (organisations or businesses), agents, foreign entities or persons conducting business in New Zealand. It generally applies to all agents conducting business on behalf of a New Zealand agency overseas.
Privacy Breach	A privacy breach can be any unauthorised access, disclosure, alteration, loss or destruction of personal information by an agency or their agent. It also includes any action that prevents access to personal information (either temporarily or permanently) by an agency or their agent. See also, *Serious Harm*.
Privacy Breach Management Plan	Wintec's Privacy Breach Management Plan. It sets out how Wintec will respond in the event there has been or is likely to be a breach of privacy of a person or persons. It is managed by the Privacy Officer and maintained by the Quality and Academic Unit.
Privacy Impact Assessment Checklist	Also known as a PIA. A series of questions answered by a project manager or relevant staff to consider the privacy implications of a new project, service, procedure, or before contracting a new service provider; the answers to which are documented and retained by QAU.
Register of Privacy Breaches	Wintec's register of privacy breaches and near misses, administered by QAU. Secure access only.
Serious Harm	Not defined in the Privacy Act 2020, however the Privacy Commissioner has said it includes physical harm or intimidation, financial fraud including unauthorised credit card transactions or credit fraud, family violence, and psychological or emotional harm. The Serious Harm Test is to be used to determine the seriousness of harm. See below.
Serious Harm Test	In the event there has been a privacy breach, a review of the breach must be completed by the Privacy Officer, consisting of six key questions: • Is the information sensitive? • What actions have been taken to reduce harm? • What is the nature of the harm? • Who has the information? • Is the information protected by a security measure? • What other relevant matters or extenuating circumstances exist? The Privacy Officer, in consultation with other relevant staff, then determines what actions to take, and whether the privacy breach is notifiable. See also, *Notifiable Privacy Breach*.
Statement of Correction	When someone submits a PIR requesting Wintec change information held about them, this is known as a Statement of Correction. If we deem the information is either already correct, or it is a matter of opinion (for example, differing accounts of the same event) then Wintec can opt not to change the personal information we have about the person. In this type of situation, we are entitled to leave the information unchanged, however we must attach the Statement of Correction along with a letter detailing why we are not making the requested change.

PRIVACY
tauākī matatapu

10. Records Management

In line with the Public Records Act 2005, Wintec is required to provide an Information and Records Management programme to ensure that authentic, reliable and usable records are created, captured and managed to a standard of best practice, and to meet business and legislative requirements. All records relevant to a specific policy need to be listed in every policy in the following format:

Record	Minimum retention period	Disposal Action	GDA Reference #
This policy document	Until superseded and administratively no longer required for reference purposes	Retail as public archive	5.1.1
Privacy Act Requests & Complaints that set precedent Records relating to requests and complaints regarding Wintec that set precedent.	10 years after date of last action	Retain as public archive	GDA 6 # 7.4.1
Privacy Act Requests & Complaints that do not set precedent Records relating to requests and complaints regarding Wintec that set no precedent.	7 years after date of last action	Destroy	GDA 6 # 7.4.2
Authority to act on behalf of a student Records related to written authority of a nominated person to act on behalf of a student.	7 years after date of last action	Destroy	2.3.1
Issue monitoring (significant) Records relating to ongoing monitoring of issues that result in significant changes to policies, procedures, strategy, risk and compliance etc., including the Register of Privacy Breaches.	10 years after date of last action	Retain as public archive	5.1.6
Issue monitoring (minor) Records relating to ongoing monitoring of issues that have no impact on policies, procedures, strategy, risk and compliance etc., including the Register of Privacy Breaches.	2 years after date of last action	Destroy	5.1.7
Administration & facilitation of complaints & issues Records that document the issue management process including the Privacy Breach Management Plan, Decision Letter, Statement of Correction and Privacy Impact Assessment Checklist	7 years after date of last action	Destroy	5.1.8

11. Version History

Version	Date Approved	Details
1	March 1996	First Published. Called *Dealing with Requests for Personal Information about Students or Staff.*
2	February 2010	Renamed *Privacy and Personal Information.* Format changed to Part A (policy) and Part B (procedures).
3	January 2017	
4	May 2021	Updated due to a change in privacy laws. Renamed Privacy. Updated template to modern template (no Part A or Part B).