GLENDOWIE SCHOOL
PRIVACY ACT PROCEDURE (updated 2021 January)

RATIONALE

To provide guidelines that will support the school in providing procedures around the implementation of our privacy policy which is in accordance with the legislative requirements of the Privacy Act 2020. These procedures relate to the Glendowie School's collection, use and disclosure of personal information.

GUIDELINES *(The following Procedures are aligned to the School Privacy Policy)* Privacy Policy and the Privacy Act Principles and Code 2020 **Appendix 1**

(It is to be understood, that the use of the word 'Parent' in this document also includes Legal Guardian or Caregiver.)

1. **PERSONAL INFORMATION COLLECTED BY THE SCHOOL**

A. Enrolment Information

- Personal Information is collected about a child as part of the application for enrolment process on the school's application form.
- Enrolment application forms can be updated at the time of **actual** enrolment, when documents verifying proof of residence, is required.
- After enrolment, or at any stage of the enrolment process, information on these forms can be requested to be updated by the school or by the parents/ caregivers of the student
- Enrolment information is able to be shared by office staff, with any teacher teaching the child and can also be shared with the Principal, SENCO, ESOL department, International staff, DP, AP or syndicate leaders.
- Parents will be required to sign the 'Use of Personal Information' form and 'Media Parent Consent' form.
- 'Use of the Cybersafety Internet' parent and student permission forms will be completed prior to taking up an enrolment position at Glendowie School ('Student Use' forms will be revisited and signed each year by the students and parents)
- Any medical forms will also be requested at the time of application, e.g. vaccination records, health forms, health management plans.
- Student application forms will be held in the archive room and data transferred to online management systems (ENROL and eTap), in order for the school to monitor attendance, student achievement and learning needs.

B. Other Information collected by the school

- Consent for immunisation forms undertaken at the school, will be obtained from parents in all cases. Consent & non consent information is collected and retained by the school health nurse on behalf of the Ministry of Health.
- Record of student achievement data collected and stored on eTap
- Permission forms for EOTC trips stored through Kindo.
- Permission and health records associated with students going on camp or overnight trips.
- Attendance data stored on the ENROL system.
- Special Needs register stored on E Tap.
- Letters of complaint/ concerns or commendations are stored in the filing cabinet in the BOT room or in committee correspondence file stored by the executive officer, if it is part of BOT correspondence.
- The school will facilitate the correction of personal information at the request of an individual. If a parent disagrees with a report/file note then a correction would occur. However, if the school is not willing to correct it as per their disagreeing with the request for change, then the parents may request that an attachment stating that they disagree with the report/ file note will be attached.

2. Disclosure of personal Information

- The school will use the template Guidelines of NZSTA **Appendix 2** outlining the procedures around requests for personal information.
- Personal Information will only be released with the permission of the two privacy officers and/or by the Deputy Principal (Acting for the Principal) and in accordance with the school policy on when the school may provide personal information.
- The school will follow agency protocols from the Ministry of Education and health agencies including RTLB, RTLit, Special Education, Kari Centre etc, for the sharing of information. In most of these instances parental permission is required before sharing this information with agencies who are seeking to support the student and their whānau
- Any person has the right to request information that the school holds about their child.
    - The school will respond as soon as practical and within 20 working days.
    - The school is aware that there could be some information which may be withheld under the Privacy Act. The school will consult with NZSTA or Privacy Commissioner or BOT lawyer in cases of uncertainty under Principle 6.
    - Requests that include the information of others will be reviewed and information that identifies or names others will be redacted.
    - See further details in: https://www.nzsta.org.nz/assets/Governance-support-resources/Responding-to-information-requests.pdf
- The Board insurer will be notified for all but straightforward information requests.
- Straightforward Privacy Act requests will go to the privacy officers. Straight forward requests under the OIA will be dealt with by the Principal. All other requests would go to the BOT.
- An information request does not have to be in writing.

3. **Holding of personal information**

- The school policy of records and school record retention and disposal policy Schools Record Retention and Disposal policy and the School Records Retention procedure will indicate the length of time personal information is held and the disposal of it.
- Disposal of information in keeping with our school record and disposal policy is through our secure bin system which is taken off site and shredded by a contracting company.

Use of photographs/videos/recordings

- Parents, at the time of enrolment, and at the time of any changes to the Media Parent Consent' form, will give written consent for the school to use their child's image or personal information.
- A document will be formed recording non-consent i.e. any student whose photo, video recordings or personal identifiable information cannot be used.
    - This will be shared with class teachers, office staff, IT Department and other staff wanting to use and display this information.
    - **A staff member publishing information or any media that identifies a student will check on this document and adhere to any publication restrictions that have been notified** e.g. Faces may be faded out or made unrecognisable in terms of a group photo if there are any restrictions filed.
- When photos/ videos / recordings are being made, the children should be told why this is occurring (This also gives them a chance to say they don't want to be part of it).
- Any outside agency e.g. news papers, promotional media will need to have parent's permission for each event.
- Student cell phones are kept at the office to help protect the privacy of individuals from filming and sharing information.

NOTIFIABLE BREACH PROCEDURES - SEE FLOW CHARTS APPENDIX

- The school will use integrity around personal information it holds and will ensure that no personal information is destroyed, knowing that a request has been made to access it.
- The school will comply with any issues or compliance notices from the Privacy Commissioner and will use this to review and amend any current practices .
- Each Board meeting the Principal will report to the BOT any breaches, notifications or near misses in terms of our commitment to the Privacy Policy and Privacy Act 2000
- The Notifiable breach form will be used for notification https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/report-a-breach/report

ROLE OF THE PRIVACY OFFICER

- Three Privacy officers, the Principal, Deputy Principal and Executive Officer will ensure that information is stored securely and access to information is monitored.
- The Privacy officers will follow the13 privacy principles.**Appendix 1**
- The Privacy Officers will follow the procedures as shown in **Appendix 3.** The privacy officers will continue to undertake professional development around their responsibilities including familiarisation with the Privacy Act, Guidelines of the Ministry of Education and NZSTA and in their review of the school privacy procedures. The elearning module

dedicated to the Privacy Act 2020 can be found on the OPC web site (this includes the ABC for schools).

Protecting Personal Information

We recognise that with technology changing very rapidly that there is a need to be looking at risks that may endanger the safety of our students and their privacy being compromised.

- Staff need to be aware of third party software Apps unless it is from a source we trust e.g. the MOE. The terms and conditions of their privacy statement need to be checked especially with free software. If the APP asks for personal information other than an initial name then it must be checked carefully so that students aren't sending out private information across the web.
- The IT department will continue to monitor safety around internet safety and students protection of personal information especially where an individual can be identified.
- Staff need to keep information safe, especially around **e-mails** where it can be sent to someone else by mistake or the email chain can be so cumbersome that confidential information/opinions are shared incorrectly.
    - It is preferable to start a new email chain and to ensure that staff recognise that this information could be accessed through a Privacy Act request. Other students' names should not be included.
    - It is better to err on the side of caution and either phone a parent or arrange an interview with them, especially if the complaint or concern involves other student's names.
    - Syndicate leaders are required to view all teacher's correspondence around a complaint and monitor the process around communication.
- Teachers will ensure that personal information about students is not left on their desks and that their computer is in privacy or lockdown mode.
- The staff room and office areas will not have information about students on display except students who have health management plans.
- Screens, printers or files are to be positioned so that they are not able to be seen by the public or unauthorised staff.
- If there is a threat in terms of a person's well being then we can disclose this information to police, social services MOE, counsellors. The information shared would only be the information disclosed and if it could lessen the threat. It would not include information not related to the threat.

Additional Procedures for Teachers

If it says 'confidential' on the form, DO NOT keep or make a copy.

Student References:

- If we are asked to supply a reference to the school we would need to be clear as to what the schools guidelines are e.g. the school wants it confidentially. So teachers may need to check with the parent or the school if you want to send it without parents seeing it.
- Be mindful that there never should be any surprises in a reference.
- The school does not keep a copy of the completed reference.

In terms of Psychologists/ counsellors.

- If a parent requests this information and is filled in by the school then the school should assume that it can give this to the parents (see privacy act).

    - The teacher has the right to know who it is going to and where it is going.
    - The teacher informs SENCO / LSC (the school does not keep a copy of the completed form) this will then alert SENCO / LSC as to a perceived need that we may not know about.
- So under the Privacy Act we will share anything with the parent if requested
    - unless it puts the child in danger e.g. abuse,
    - unless requested under statutory law e.g. Oranga Tamariki, police,
    - or as above if it's a confidential form for Kari Centre.

The Kari Centre (Auckland DHB mental health) and Oranga Tamariki

- If the Kari Centre sends us a referral form to fill in and return to them then we will do this.
    - If a parent requests to see the form we have sent to the Kari Centre then we would advise them to contact the Kari Centre or we can contact the Kari Centre to send us a copy that we can forward to the parent.
    - We don't keep a copy but that SENCO / LSC can read it before it is sent off to familiarise herself with what has been sent.
    - The original referral may even have come from the school.
    - SENCO / LSC could then make a suitable note on the school file, that it was sent,or any brief note needed, remembering the parent can ask to see any information we hold on a child (except in cases e.g. of abuse)
- (The Kari Centre will accept referrals from any professional involved in the young person's care.
    - There is an expectation that the referrer has discussed the problem with the student's and their family/whanau.
    - Once the referral has been received, the Kari Centre may make contact with the referrer to discuss the case or gather more information.

Privacy Act FAQ

WHAT INFORMATION MAY PARENTS RECEIVE ABOUT THEIR CHILD?

- Principle 6 Access to personal information: This provides that individuals concerned are entitled to know whether the agency (this means the BOT and through them the employees who are liable to uphold the Boards' policies) holds such personal information, and if so, can have access to that information and may request correction of the information.
- Do parents have a right to access personal information about their children? The Privacy Act provides amongst other things for access by individuals to information about themselves. Thus, under the Privacy Act, it is the child who has the right to access their own information. Exceptions exist where there are statutory rights of access given to parents.
- A clear example of such a right is section 77 (b) of the Education Act 1989 which requires the principal to tell a student's parents: "…of matters that, in the principal's opinion: (i) are preventing or slowing the student's progress through the school, or (ii) are harming the student's relationships with teachers or other students." Parents must be given such information.

- There may be occasions when the child's right to privacy would clearly outweigh any interest in providing access to the information to the parent's. Such an occasion would include where the child is alleging abuse by the parents.
- Even where the facts might lead the school to decide against giving access to all information requested by the parents, it should consider whether it is possible to give access to part of the information, deleting the information raising the particular concern.
- Can a principal provide personal information to a specialist service? The information provided to the specialist service has been collected for education purposes and to meet the requirements of section 77 (a). Passing this information to the specialist service for assistance to deal with problems related to the education of a student can be seen as one of the purposes for which this information was collected. It therefore fits within principle 11.
- Parents may request that information. A relevant section in considering such a request is section 53(b) of the Privacy Act, which allows an agency to refuse disclosure where the disclosure of the information would involve the unwarranted disclosure of the affairs of another person, e.g.the student.Also consider section 49 of the Privacy Act, which allows an agency to refuse disclosure if that would be likely among other things to endanger the health or safety of any individual. (Check section 49 carefully and seek advice if necessary if that section may apply)

APPENDIX 1

Information 12 privacy principles and section 22 of the Privacy Act 2020

The information privacy principles are as follows:

1 Purpose of collection of personal information

(1) Personal information must not be collected by an agency unless— (a) the information is collected for a lawful purpose connected with a function or an activity of the agency; and (b) the collection of the information is necessary for that purpose. (2) If the lawful purpose for which personal information about an individual is collected does not require the collection of an individual's identifying information, the agency may not require the individual's identifying information.

2. **Information privacy principle. Source of personal information**

(1) If an agency collects personal information, the information must be collected from the individual concerned. (2) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,— (a) that non-compliance would not prejudice the interests of the individual concerned; or (b) that compliance would prejudice the purposes of the collection; or (c) that the individual concerned authorises collection of the information from someone else; or (d) that the information is publicly available information; or (e) that non-compliance is necessary— (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or (ii) for the enforcement of a law that imposes a pecuniary penalty; or (iii) for the protection of public revenue; or (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or (v) to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual; or (f) that compliance is not reasonably practicable in the circumstances of the

particular case; or (g) that the information— (i) will not be used in a form in which the individual concerned is identified; or (ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

3. Collection of information from subject

(1)If an agency collects personal information from the individual concerned, the agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of— (a) the fact that the information is being collected; and (b) the purpose for which the information is being collected; and (c) the intended recipients of the information; and (d) the name and address of— (i) the agency that is collecting the information; and (ii) the agency that will hold the information; and (e) if the collection of the information is authorised or required by or under law,— (i) the particular law by or under which the collection of the information is authorised or required; and (ii) whether the supply of the information by that individual is voluntary or mandatory; and (f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and (g) the rights of access to, and correction of, information provided by the IPPs. (2) The steps referred to in subclause (1) must be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected. (3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if the agency has taken those steps on a recent previous occasion in relation to the collection, from that individual, of the same information or information of the same kind. (4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,— (a) that non-compliance would not prejudice the interests of the individual concerned; or (b) that non-compliance is necessary— (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or (ii) for the enforcement of a law that imposes a pecuniary penalty; or (iii) for the protection of public revenue; or (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or (c) that compliance would prejudice the purposes of the collection; or (d) that compliance is not reasonably practicable in the circumstances of the particular case; or (e) that the information— (i) will not be used in a form in which the individual concerned is identified; or (ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

4. Manner of collection of personal information

An agency may collect personal information only— (a) by a lawful means; and (b) by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons), (i) is fair; and (ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

5. Storage and security of personal information

An agency that holds personal information must ensure— (a) that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against— (i) loss; and (ii) access, use, modification, or disclosure that is not authorised by the agency; and (iii) other misuse; and (b) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

6. Access to personal information

(1) An individual is entitled to receive from an agency upon request— (a) confirmation of whether the agency holds any personal information about them; and (b) access to their personal information. (2) If an individual concerned is given access to personal information, the individual must be advised that, under IPP 7, the individual may request the correction of that information. (3) This IPP is subject to the provisions of Part 4. Information privacy principle

7 **Correction of personal information**

(1)An individual whose personal information is held by an agency is entitled to request the agency to correct the information. (2) An agency that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading. (3) When requesting the correction of personal information, or at any later time, an individual is entitled to.(a) provide the agency with a statement of the correction sought to the information (a statement of correction); and (b) request the agency to attach the statement of correction to the information if the agency does not make the correction sought. (4) If an agency that holds personal information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information. (5) If an agency corrects personal information or attaches a statement of correction to personal information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information. (6) Subclauses (1) to (4) are subject to the provisions of Part 4.

8. Accuracy, etc, of personal information to be checked before use or disclosure

An agency that holds personal information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

9. Agency not to keep personal information for longer than necessary

An agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

10.Limits on use of personal information

(1) An agency that holds personal information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency believes, on reasonable grounds,— (a) that the purpose for which the information is to be used is directly related to the purpose in connection with which the information was obtained; or (b) that the information— (i) is to be used in a form in which the individual concerned is not identified; or (ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or (c) that the use of the information for that other purpose is authorised by the individual concerned; or (d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or (e) that the use of the information for that other purpose is necessary— (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or (ii) for the enforcement of a law that imposes a pecuniary penalty; or (iii) for the protection of public revenue; or (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or

are reasonably in contemplation); or (f) that the use of the information for that other purpose is necessary to prevent or lessen a serious threat to— (i) public health or public safety; or (ii) the life or health of the individual concerned or another individual. (2) In addition to the uses authorised by subclause (1), an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.

11. Limits on disclosure of personal information

1. An agency that holds personal information must not disclose the information to any other agency or to any person unless the agency believes, on reasonable grounds,— (a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or (b) that the disclosure is to the individual concerned; or (c) that the disclosure is authorised by the individual concerned; or (d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or (e) that the disclosure of the information is necessary— (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or (ii) for the enforcement of a law that imposes a pecuniary penalty; or (iii) for the protection of public revenue; or (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or (f) that the disclosure of the information is necessary to prevent or lessen a serious threat to— (i) public health or public safety; or (ii) the life or health of the individual concerned or another individual; or (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or (h) that the information— (i) is to be used in a form in which the individual concerned is not identified; or (ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or (i) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern. (2) This IPP is subject to IPP 12

12. Disclosure of personal information outside New Zealand

(1) An agency (A) may disclose personal information to a foreign person or entity (B) in reliance on IPP 11(1)(a), (c), (e), (f), (h), or (i) only if— (a) the individual concerned authorises the disclosure to B after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in this Act; or (b) B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to this Act; or (c) A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in this Act; or (d) A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or (e) A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or (f) A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in this Act (for example, pursuant to an agreement entered into between A and B). (2) However, subclause (1) does not apply if the personal information is to be disclosed to B in reliance on IPP 11(1)(e) or (f) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subclause (1). (3) In this IPP,— prescribed binding scheme means a binding scheme specified in regulations made under section 213 prescribed country means a country specified in regulations made under section 214.

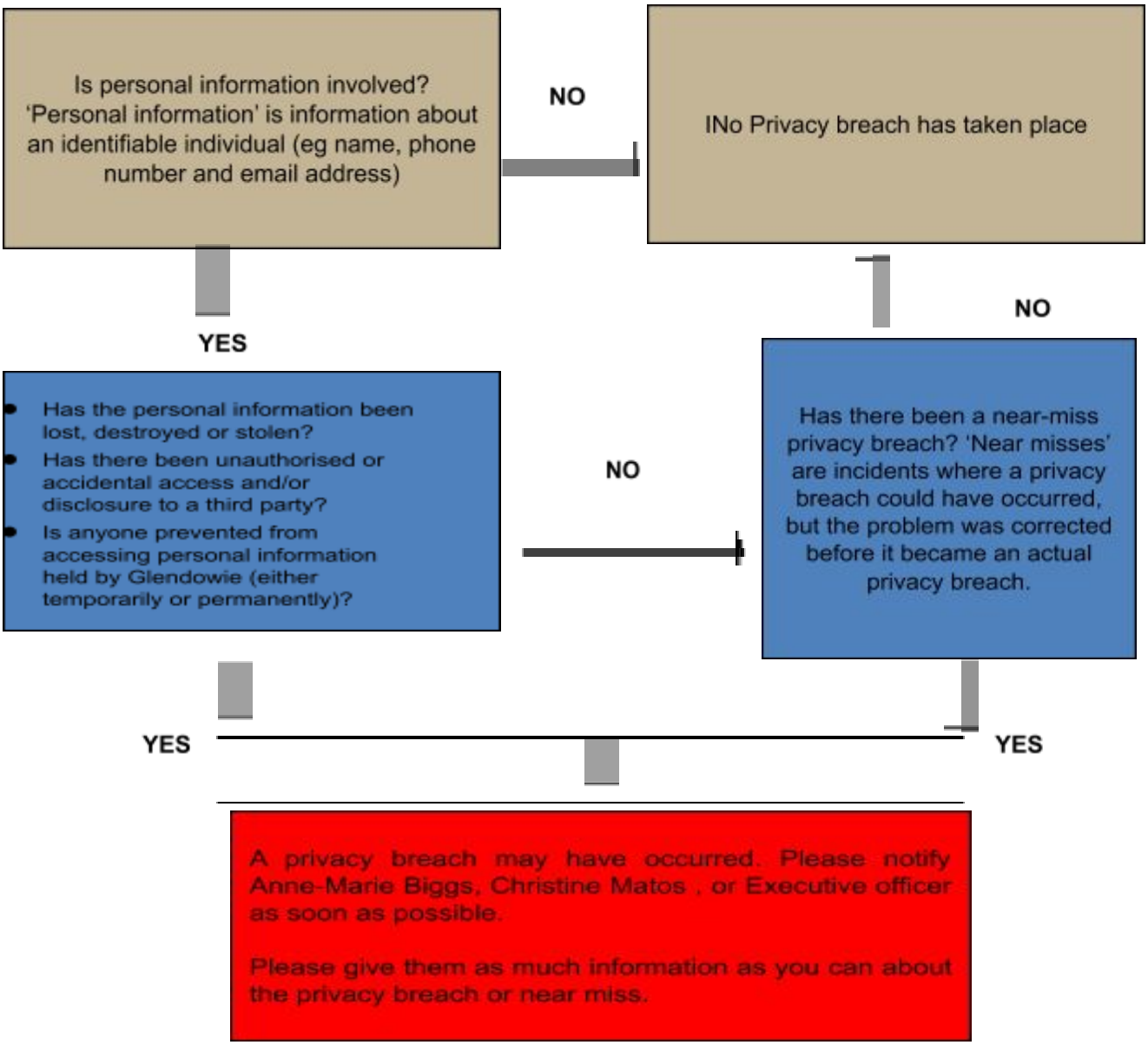
13. Unique identifiers

(1) An agency (A) may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable A to carry out 1 or more of its functions efficiently. (2) A may not assign to an individual a unique identifier that, to A's knowledge, is the same unique identifier as has been assigned to that individual by another agency (B), unless— (a) A and B are associated persons within the meaning of subpart YB of the Income Tax Act 2007; or (b) the unique identifier is to be used by A for statistical or research purposes and no other purpose. (3) To avoid doubt, A does not assign a unique identifier to an individual under subclause (1) by simply recording a unique identifier assigned to Reprinted as at 9 December 2020 Privacy Act 2020 Part 3 s 22 31 the individual by B for the sole purpose of communicating with B about the individual. (4) A must take any steps that are, in the circumstances, reasonable to ensure that— (a) a unique identifier is assigned only to an individual whose identity is clearly established; and (b) the risk of misuse of a unique identifier by any person is minimised (for example, by showing truncated account numbers on receipts or in correspondence). (5) An agency may not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or is for a purpose that is directly related to one of those purposes.

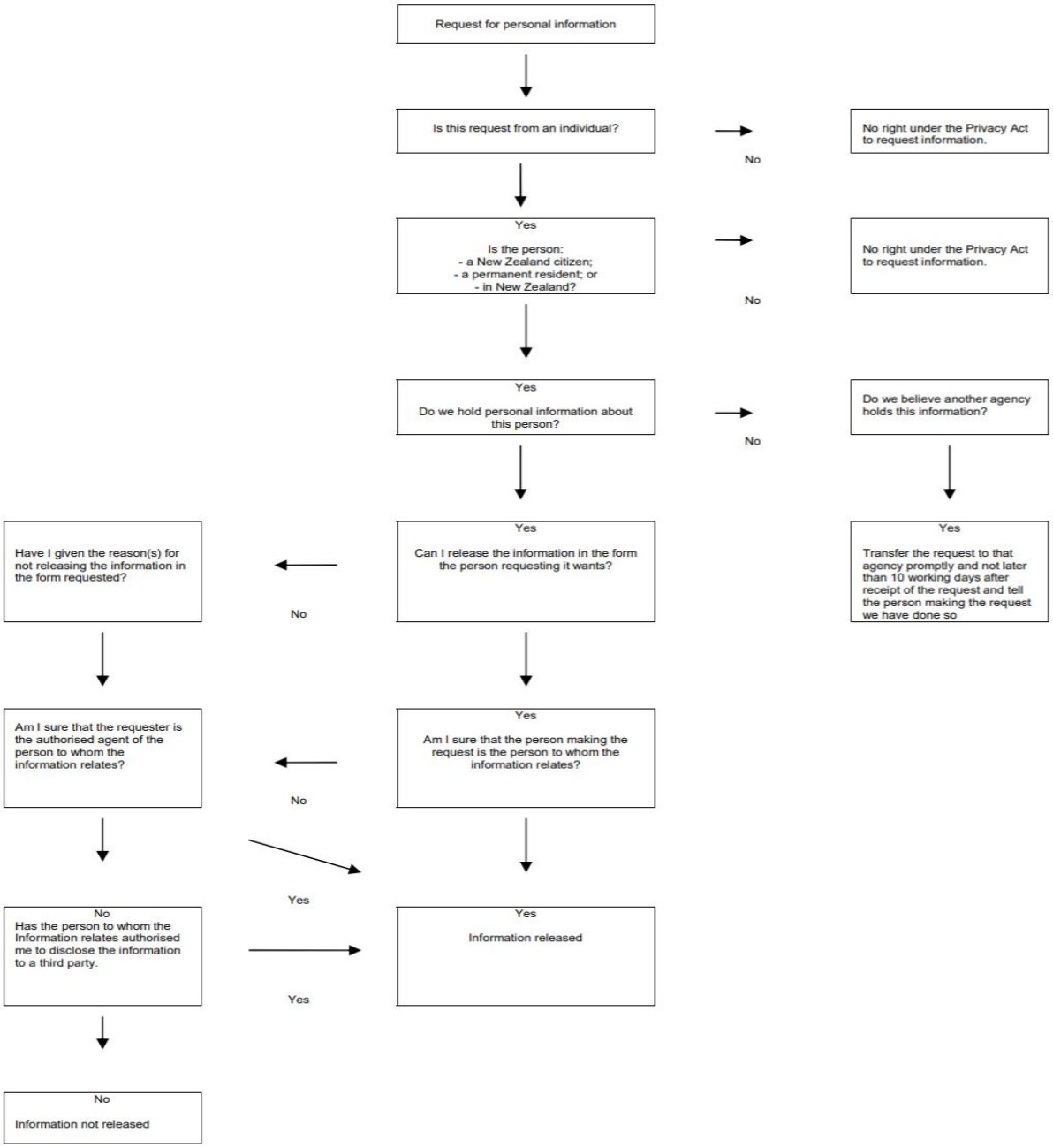
APPENDIX 4: PRIVACY BREACH PROCESS

Glendowie School is committed to protecting personal information and ensuring that we respond appropriately to privacy breaches involving our staff, students or community.

The flow chart below is to help you understand what to do if you think an actual or 'near miss' privacy breach has occurred. If you are unsure about whether a privacy breach or near miss has taken place, please tell the Principal, Deputy Principal or Chief Executive Officer as soon as possible so that we can properly assess what has happened and take appropriate action.

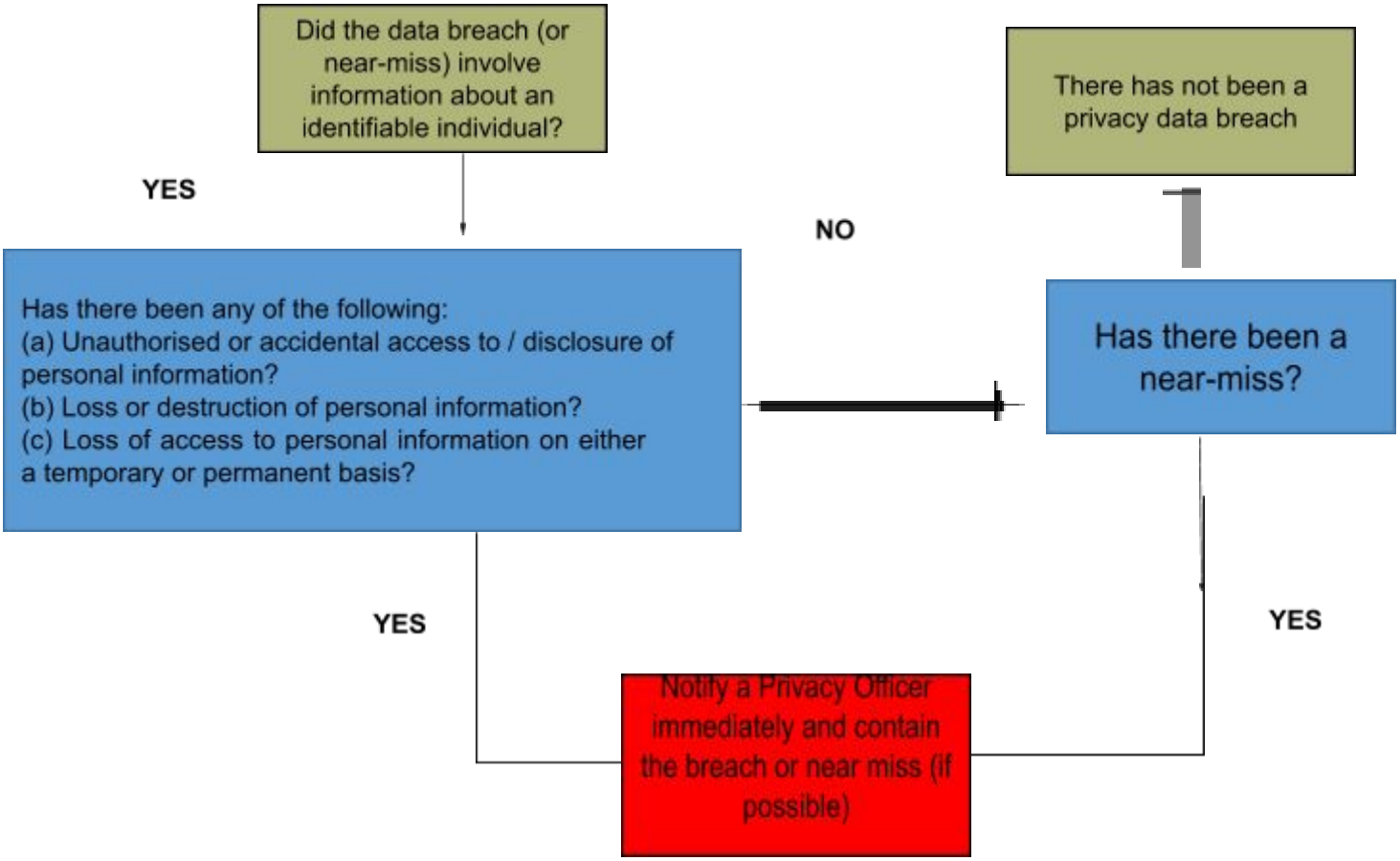


APPENDIX 2: REQUESTS FOR PERSONAL INFORMATION FLOWCHART

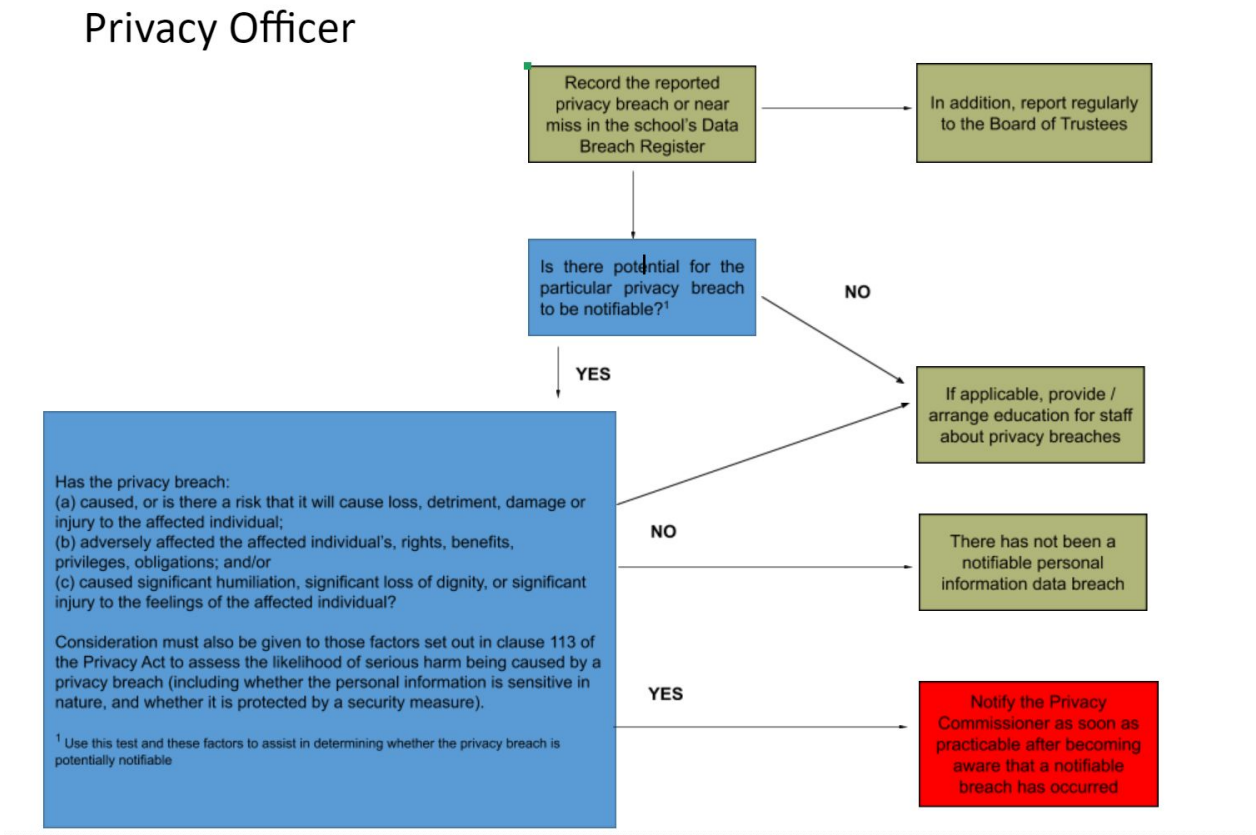


APPENDIX 5

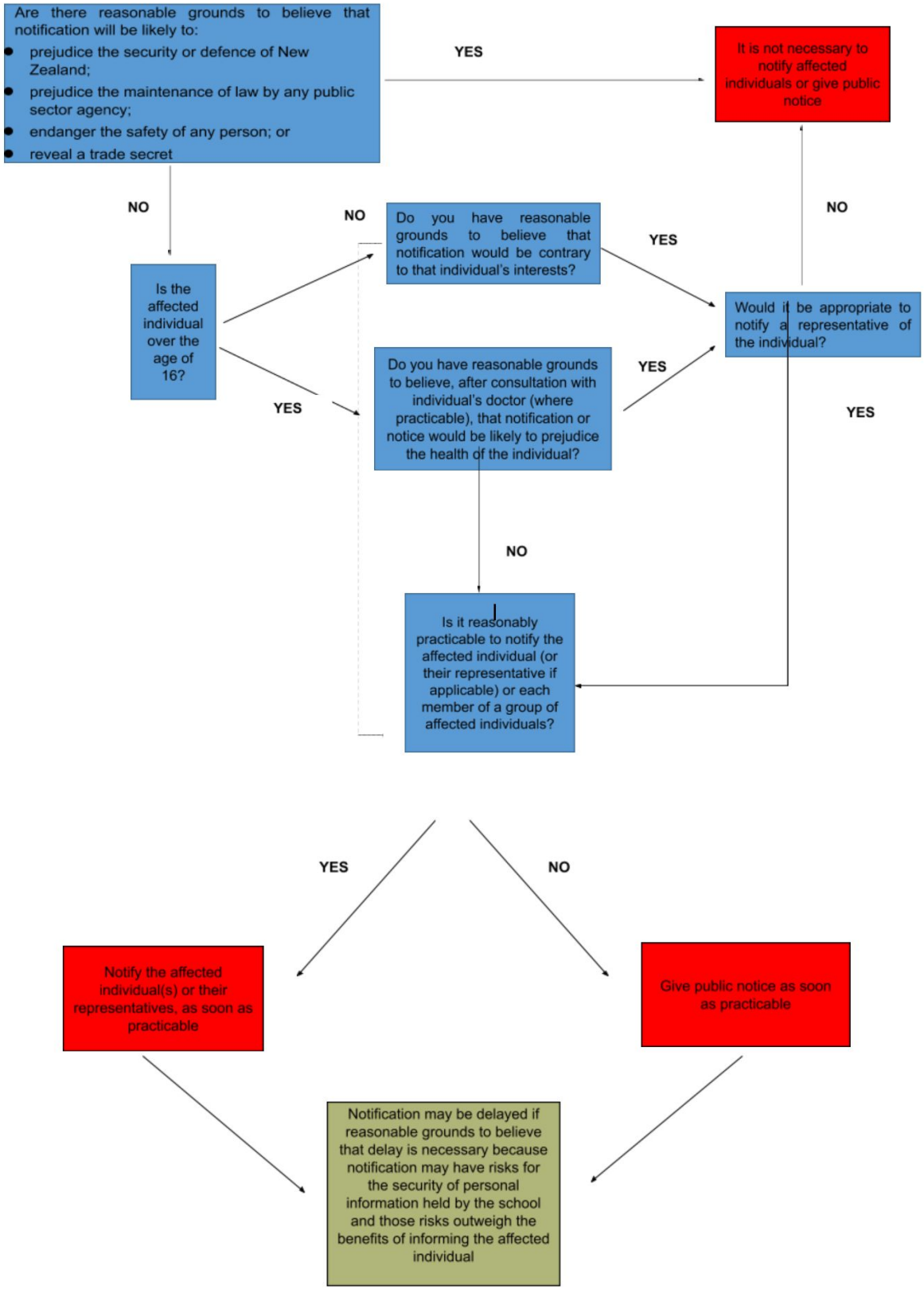
Staff



APPENDIX 3



In addition to notifying the Privacy Commissioner, Glendowie School may have to notify the affected individual(s) (or their representative) or give public notice


Are there reasonable grounds to believe that notification will be likely to:
prejudice the security or defence of New Zealand;
prejudice the maintenance of law by any public sector agency;
endanger the safety of any person; or
reveal a trade secret
YES
It is not necessary to notify affected individuals or give public notice
NO
NO
Do you have reasonable grounds to believe that notification would be contrary to that individual's interests?
YES
NO
Is the affected individual over the age of 16?
Would it be appropriate to notify a representative of the individual?
YES
Do you have reasonable grounds to believe, after consultation with individual's doctor (where practicable), that notification or notice would be likely to prejudice the health of the individual?
YES
YES
NO
Is it reasonably practicable to notify the affected individual (or their representative if applicable) or each member of a group of affected individuals?
YES
NO
Notify the affected individual(s) or their representatives, as soon as practicable
Give public notice as soon as practicable
Notification may be delayed if reasonable grounds to believe that delay is necessary because notification may have risks for the security of personal information held by the school and those risks outweigh the benefits of informing the affected individual