PRIVACY POLICY

Title	3.10-009 Privacy Policy
Category	Administration
Policy Owner	Executive Committee
Approver	Board of Directors
Related Documents	• *Privacy Act 1988 (Cth)* • *Privacy Amendment (Enhancing Privacy Protection) Act 2012* • 1.20-006 Mueller College Child Protection Policy • 1.20-008 Mueller College Disability Discrimination Policy • Mueller College Data Breach Policy (see Appendix 9)
Published Location	*Internal* Dropbox > Policies & Procedures > 3 – Administration > 3.10 Administration *External* Mueller College Website

Revision Record					
Version	**Approval Date**	**Approved By**	**Effective Date**	**Review Cycle**	**Next Review**
March 2015	March 2015		March 2015	Annual	2016
January 2016	January 2016		January 2016	Annual	2017
January 2017	January 2017		January 2017	Annual	2018
February 2018	February 2018		February 2018	Annual	2019
January 2019	January 2019		January 2019	Annual	2020
V21.3	March 2021	Board of Directors	March 2021	Annual	2022
V22.5	May 2022	Board of Directors	May 2022	Annual	2023
V23.1	January 2023	Board of Directors	January 2023	Annual	2024
V24.3	March 2024	Board of Directors	March 2024	Annual	2025

1. Purpose and Scope

1.1 Mueller College is bound by the Australian Privacy Principles contained in the *Privacy Act 1988 (Cth)*. This statement outlines the privacy policy of the school and describes how the school uses and manages personal information provided to or collected by it.

1.2 The policy applies to board members, employees, volunteers, parents/guardians and students, contractors, and people visiting the school site; and describes the type of information the school collects, how the information is handled, how and to whom the information is disclosed, and how the information may be accessed.

2. Exemption in Relation to Employee Records

2.1 Under the *Privacy Act 1998 (Cth)* ("Privacy Act"), the Australian Privacy Principles do not apply to an employee record held by the employing entity. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and employee.

3. Introduction

3.1 A Privacy Policy is needed to inform individuals about the practices of the School in relation to personal information. It also serves as a guide to the School's staff as to the standards to be applied in respect of handling personal information and ensure consistency in the School's approach to privacy.

3.2 'Personal information' within the meaning of the Privacy Act includes information or an opinion about an identified individual (or an individual who is reasonably identifiable). Personal information may also be classified as sensitive information or health information, as defined by the Privacy Act.

3.3 Sensitive information includes information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

3.4 The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

4. What Kinds of Personal Information Does the School Collect and How Does the School Collect It?

4.1 The type of information the School collects and holds includes (but is not limited to) personal information, including health and other sensitive information, about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the School;
- job applicants, staff members, volunteers and contractors; and
- other people who come into contact with the School.

4.2 **Personal Information you provide** - The School will generally collect personal information held about an individual by way of forms filled out by Parents or pupils, face-to-face meetings and

interviews, emails and telephone calls. On occasions people other than Parents and pupils provide personal information.

4.3 **Personal Information provided by other people** - In some circumstances the School may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a transfer note from another school.

4.4 Collection of Sensitive Information – We only collect sensitive information if it is:

- reasonably necessary for the School's functions and activities;
- reasonably necessary for the School's functions and activities, with the individual's consent;
- necessary to lessen or prevent a serious threat to health and safety;
- another permitted general situation; or
- another permitted health situation.

5. How Does the School Use Personal Information?

5.1 The School will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected by you, or to which you have consented.

6. Pupils and Parents

6.1 In relation to personal information of pupils and Parents, the School's primary purpose of collection is to enable the School to provide schooling for the pupil. This includes satisfying the needs of Parents, the needs of the pupil and the needs of the School throughout the whole period the pupil is enrolled at the School.

6.2 The School's primary uses of personal information of pupils and parents for the purpose of providing schooling to the pupil includes:

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration of the School;
- looking after pupils' educational, social, spiritual and medical wellbeing;
- marketing, promotional and fundraising activities; and
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

6.3 In some cases where the School requests personal information about a pupil or Parent, if the information requested is not provided, the School may not be able to enrol or continue the enrolment of the pupil, or permit the pupil to take part in a particular activity.

7. Job Applicants, Staff Members and Contractors

7.1 In relation to personal information of job applicants, staff members and contractors, the School's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be.

7.2 Uses of personal information of job applicants, staff members and contractors for that primary purpose will include:

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- marketing, promotional and fundraising activities; and

- satisfying the School's legal obligations, for example, in relation to work health and safety and child protection legislation.

7.3 Personal information including sensitive information of staff members and contractors will be disclosed to Redcliffe Assembly (as the legal entity which employs staff at Mueller College) and Mueller Community Church for the purposes described above.

8. Volunteers

8.1 The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as alumni associations, to enable the School and the volunteers to work together.

9. Marketing and Fundraising

9.1 The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to provide a quality learning environment in which both pupils and staff thrive.

Personal information (but not sensitive or health information) held by the School may be disclosed to organisations that assist in the School's fundraising, for example, the School's Foundation or alumni organisation or, on occasions, external fundraising organisations.

9.2 You may request that the College does not disclosure your personal information for marketing and fundraising purposes by contacting admin@mueller.qld.edu.au

9.3 Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes. A student photo or media item may be used for marketing. Please let the school know if you do not wish this to occur.

10. Who Might the School Disclose Personal Information To?

10.1 The School may disclose personal information about an individual, including sensitive information, for purposes directly related to the primary purpose for collection, or for a secondary purpose where you have provided consent or would otherwise reasonably expect the personal information to be disclosed in that manner.

10.2 Information may be disclosed to:

- another school (upon receipt of a transfer note or otherwise by consent);
- Mueller Community Church, including Mueller College Early Learning Centre (MCELC) and Mueller College Outside School Hours Care (MCOSHC);
- government departments;
- medical practitioners;
- people providing services to the School, including specialist visiting teachers, counsellors and sports coaches;
- recipients of School publications, such as newsletters and magazines;
- Parents;
- The school's alumni association pursuant to Appendix 3;
- anyone you authorise the School to disclose information to; and
- anyone to whom we are required to disclose the information to by law.

10.3 Where information is disclosed to Mueller Community Church (MCC), that information may be used for the following purposes:

- To comply with the legal obligations of MCELC and MSOSHC and allow MCC to discharge its duty of care in the operation of the Church and its services;
- To allow for day-to-day administration of MCELC and MCOSHC;
- To effectively look after children's educational, social and medical wellbeing; and
- To keep parents informed about matters related to their child through correspondence, newsletters etc.

10.4 Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

11. Sending Information Overseas

11.1 The School may disclose personal information about an individual to overseas recipients, for instance, when storing personal information with 'cloud' service providers which are situated outside Australia or to facilitate a school exchange. This may include trusted sites such as 'Edmodo' and 'Google Docs'.

11.2 However, otherwise, the School will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- satisfying ourselves that the overseas recipient is compliant with the APPs, or a similar privacy regime.

12. Management and Security of Personal Information

12.1 The School's staff are required to respect the confidentiality of pupils' and Parents' personal information and the privacy of individuals. The School has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records. It is College policy to maintain complete student files indefinitely.

12.2 On 22 February 2018 new 'data breach' privacy laws came into effect. Under these laws action must be taken if there has been an 'eligible data breach'.

13. Access and Correction of Personal Information

13.1 Under the Privacy Act, an individual has the right to obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy.

13.2 Pupils will generally be able to access and update their personal information through their Parents, but older pupils may seek access and correction themselves. The School will consider any such requests from students on a case by case basis, taking into account the student's age and maturity, and the nature of the information in question.

13.3 There are some exceptions to these rights set out in the applicable legislation.

13.4 To make a request to access or update any personal information the School holds about you or your child, please contact the Head of College in writing. The School may require you to verify your

identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

14. Consent and Rights of Access to the Personal Information of Pupils

14.1 The School respects every Parent's right to make decisions concerning their child's education. Generally, the School will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's Parents. The School will treat consent given by Parents as consent given on behalf of the pupil, and notice to Parents will act as notice given to the pupil.

14.2 As mentioned above, parents may seek access to personal information held by the School about them or their child by contacting the Head of College. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the pupil.

14.3 The School may, at its discretion, on the request of a pupil grant that pupil access to information held by the School about them, or allow a pupil to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the pupil and/or the pupil's personal circumstances so warranted.

15. Enquiries and Complaints

15.1 If you would like further information about the way the School manages the personal information it holds, or wish to complain that you believe that the School has breached the Australian Privacy Principles please contact the Head of College. The School will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

Appendix 1 - Summary of Key Changes

Version	Key Changes
V21.3	Revised by Corney & Lind. Whole document reviewed, but specifically updated to include inter-entity information sharing details (Section 10)

Appendix 2 - Standard Collection Notice

1. The School collects personal information, including sensitive information about pupils and parents or guardians before and during the course of a pupil's enrolment at the School. This may be in writing or in the course of conversations. The primary purpose of collecting this information is to enable the School to provide schooling to the pupil and to enable them to take part in all the activities of the School.
2. Some of the information we collect is to satisfy the School's legal obligations, particularly to enable the School to discharge its duty of care.
3. Laws governing or relating to the operation of a school require certain information to be collected and disclosed. These include relevant Education Acts, and Public Health and Child Protection laws.
4. Health information about pupils is sensitive information within the terms of the Australian Privacy Principles under the Privacy Act. We may ask you to provide medical reports about pupils from time to time.
5. The School from time to time discloses personal and sensitive information to others for administrative and educational purposes, including to facilitate the transfer of a pupil to another school. This includes to other schools, government departments, medical practitioners, and people providing services to the School, including specialist visiting teachers, coaches, volunteers and counsellors.
6. Personal information collected from pupils is regularly disclosed to their parents or guardians.
7. Generally the School does not store personal information in the 'cloud' outside Australia. There are limited occasions when cloud storage may involve servers situated outside Australia, in which case appropriate data handling and security arrangements are in place - as required in Australia.
8. The School's Privacy Policy sets out how parents or pupils may seek access to personal information collected about them. However, there will be occasions when access is denied. Such occasions would include where access would have an unreasonable impact on the privacy of others, where access may result in a breach of the School's duty of care to the pupil, or where pupils have provided information in confidence.
9. The School Privacy Policy also sets out how you may complain about a breach of privacy and how the School will deal with such a complaint.
10. As you may know the School from time to time engages in fundraising activities. Information received from you may be used to make an appeal to you. It may also be disclosed to organisations that assist in the School's fundraising activities solely for that purpose. We will not disclose your personal information to third parties for their own marketing purposes without your consent. Provision is also made for individuals to opt-out from direct marketing.
11. On occasions information such as academic and sporting achievements, pupil activities such as school camps and excursions and similar news is published in School newsletters, magazines and on our online media channels. This may include photographs and video clips.
12. We may include pupils' and pupils' parents' contact details in a class list and School directory.
13. If you provide the School with the personal information of others, such as doctors or emergency contacts, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish and that the School does not usually disclose this information to third parties.

Appendix 3 - Alumni Association Collection Notice

1. The Alumni Association may collect personal information about you from time to time. The primary purpose of collecting this information is to enable us to inform you about our activities and the activities of Mueller College and to keep alumni members informed about other members.
2. We must have the information referred to above to enable us to continue your membership of the Alumni Association.
3. As you know, from time to time we engage in fundraising activities. The information received from you may be used to make an appeal to you. It may also be used by Mueller College to assist in its fundraising activities. If you do not agree to this, please advise us now.
4. The Alumni Association may publish details about you in our Alumni magazine and our School's website. If you do not agree to this you must advise us now.
5. The School's Privacy Policy contains details of how you may seek access to personal information collected about you or how you may complain about a breach of the APPs.
6. The School may store personal information in the 'cloud' - which may mean that it resides on servers which are situated outside Australia.
7. If you provide personal information to us about other people, we encourage you to inform them of the above matters.

Appendix 4 - Employment Collection Notice

1. In applying for this position you will be providing Mueller College with personal information. We can be contacted at:
   Mueller College Ltd, PO Box 487, Redcliffe, QLD 4020.
   Email: admin@mueller.qld.edu.au;
   Phone: 3897 2990.
2. If you provide us with personal information, for example, your name and address or information contained on your resume, we will collect the information in order to assess your application for employment. We may keep this information on file if your application is unsuccessful in case another position becomes available.
3. The School's Privacy Policy contains details of how you may complain about a breach of the APPs or how you may seek access to personal information collected about you. However, there may be occasions when access is denied. Such occasions would include where access would have an unreasonable impact on the privacy of others.
4. We will not disclose this information to a third party without your consent.
5. We may use the information you have provided to conduct a criminal record check, collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences under Child Protection laws. We may also collect personal information about you in accordance with these laws.
6. The School may store personal information in the 'cloud' - which may mean that it resides on servers which are situated outside Australia.
7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish and that the School does not usually disclose the information to third parties.
8. If your application is successful, you consent to us sharing personal information with Redcliffe Assembly (as the legal entity which employs staff at Mueller College) and Mueller Community Church for the purpose of administrative and legal requirements in relation to your employment.

Appendix 5 - Contractor/Volunteer Collection Notice

1. In applying to provide services to the School, you will be providing Mueller College with personal information. We can be contacted at:
   Mueller College Ltd, PO Box 487, Redcliffe, QLD 4020.
   Email: admin@mueller.qld.edu.au;
   Phone: 3897 2990.
2. If you provide us with personal information, for example your name and address or information contained on your resume, we will collect the information in order to assess your application. We may also make notes and prepare a confidential report in respect of your application.
3. You agree that we may store this information for 12 months.
4. The School's Privacy Policy sets out how you may seek access to your personal information and how you may complain about a breach of the APPs.
5. We will not disclose this information to a third party without your consent.
6. We are required to conduct a criminal record check, collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences under Child Protection laws. We may also collect personal information about you in accordance with these laws.
7. The School may store personal information in the 'cloud' - which may mean that it resides on servers which are situated outside Australia.
8. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish and that the School does not usually disclose the information to third parties.

Appendix 6 - Disclosure Statement to Students

Counselling at Mueller College – Things You Should Know

The College provides counselling services for its students as part of its pastoral care program. These are provided through counsellors employed by the College.

Students are encouraged to make use of these services if they need assistance. There are however a number of things that students and their parents should know before using the counselling service.

1. Records will be made of counselling sessions and because the counsellor is an employee, those records belong to the school, not the counsellor.
2. The School is very conscious of the need for confidentiality between counsellor and student. However at times it may be necessary for the Counsellor to divulge the contents of discussions or records to the Head of College if the Head of College or the Counsellor considers it necessary for the student's welfare to discharge the school's duty of care to the student.
3. It is also possible that the Head of College may need to disclose aspects of discussions with counsellors to others in order to assist the student.
4. Where a disclosure is made it would be limited to those who need to know, unless the student consents to some wider disclosure.

We emphasise that disclosures (if any) would be very limited. However if a student is not prepared to use the counselling services on the basis set out above the student will need to obtain counselling services from outside the school.

Appendix 7 - Summary - Privacy Planning - Mueller College

Table 1 - Summary - Collection - Items of Information

What	Circumstances	Place/Method	Time	Storage
Student Details Personal (includes address, email address), medical, family/guardian, educational info	For enrolment, on-going education	School Various methods - hard copy, phone, electronic, face to face	Any time through year	Secured hard storage; Electronic (eg TASS) [Sydney]
Staff Details Personal, medical, financial (eg TFB, bank accounts)	For employment	School Various methods - hard copy, phone, electronic etc.	Any time through year	Secured hard storage; Electronic (pay software)
Parental/Guardian Personal, financial, contact numbers, emergency numbers	For child enrolment, on-going education	School Various methods - hard copy, phone, electronic etc.	Any time through year	Secured hard storage; Electronic (eg TASS) [Sydney]
Volunteer Details Personal, medical	For help at school	Via school forms or electronic media	Prior to work at school	Secured hard storage; Electronic (secured computer network drives) [Dropbox]
Contractors and Suppliers: Name, address, contact information, WHS info (WorkCover/ insurance details, work method statements), company details	To perform contract work at school; supply of products	Hard copy, phone, electronic etc.	When services procured; WHS info annually	Secured hard storage; Electronic (secured computer network drives) [Dropbox]

Appendix 8 - Miscellaneous Issues

BYOD - Portable Electronic Devices

BYOD or Bring Your Own Device refers to the practice where staff use their own personal devices (such as smartphones and tablets) for work-related purposes. The considerations below also apply to College- owned portable devices such as iPads and laptops at Mueller College.

The use of personal devices for work purposes has numerous benefits for employers and employees alike, such as the lift in productivity for companies and increased flexibility and convenience for staff.

Aside from allowing staff to check their emails and calendars while they are out of the office, staff are able to work faster when working on devices they are more familiar with, such as their own.

But the benefits portable devices bring to employers also come along with a raft of risks that range from issues of data security, human resources to intellectual property.

The use of portable devices means that risks that once remained only an issue in the physical workplace are now a risk wherever they can be used – and that is just about anywhere. That means companies could be exposed to a range of risks that occur outside the workplace, such as being potentially liable for the conduct of an employee whenever they use their BYOD or an employee's smartphone being hacked into by malicious software.

At least eight categories of potential risk are identified, which include:

- Data security, where company IT security could be breached via a BYOD.
- Privacy, where the privacy of work colleagues and clients need to be respected at all times.
- Confidentiality, where company information can be exposed by devices being used in public.
- Resignation of a staff member, where company information is still stored on a BYOD.
- Legal liability, which can relate to intellectual property issues or whether a device can be used in illegal activity.
- Lost/stolen devices, which could expose company data.
- Compatibility of devices, where not all BYODs may be compatible with the workplace IT system.
- Costs, which relates to the cost of supporting, maintaining and data costs of a BYOD.

At Mueller College the IT Use Policy articulates how computers including personal and portable devices should be used by staff. This includes:

- Security of devices and data privacy.
- Network Usage.
- Copyright Regulations.
- User Agreement.

The User Agreement must be signed by staff prior to using their device as an acknowledgement that they understand the implications and their responsibilities in accessing company information.
On induction, staff are also required to sign a statement committing to confidentiality of information encountered during their employment.

Digital Photocopiers and Multi-Function Printers

Inadvertent Collection and Storage of Personal Information

Most digital photocopiers and MFPs now incorporate a digital scanner and a high-capacity hard drive which can store thousands of scanned images. Many such devices save and store scanned images created in the process of making copies, scanning documents, emailing or sending faxes. Businesses that offer photocopying or scanning services may be inadvertently collecting large amounts of personal information from their clients.

Similarly, any agency or organisation whose employees use office facilities to scan or copy personal information may be inadvertently accumulating and storing that information. Agencies and organisations that collect personal information, deliberately or inadvertently, may be subject to obligations under the Privacy Act in respect of the handling of that information.

['Personal information' within the meaning of the Privacy Act includes any document that contains information that can be linked with a person's identity].

Mueller College procedure when buying or leasing a new photocopier or MFP:

- ask the manufacturer or supplier about the options available with respect to privacy and information security - preferably to automatically delete or overwrite scanned images once copying or scanning operations are completed;
- networked devices are protected behind a 'firewall', so that they cannot be accessed via the internet by unauthorised persons;
- ensuring that a device capable of sending scanned images by email, is configured to send email to authorised accounts only (such as internal office email accounts);
- ensuring that personal information is not disclosed when selling, returning, or disposing of a photocopier or MFP.

Appendix 9 - Data Breach Policy

INTRODUCTION

The School maintains the privacy of personal information about staff, students and family members through the following means:

- Containing personal information in an access controlled Student Information System (TASS).
- Protecting data in the Student Information System and its database through appropriate backups.
- Controlling and discouraging users from copying or sharing information from the Student Information System.
- Encouraging responsible security and password behaviours among staff with access to personal information.
- Physically securing computers to prevent direct unauthorised access.

DEFINITIONS

The School is obliged to act when there has been an 'eligible data breach' involving:

- unauthorised access, disclosure or loss of personal information
- that may result in serious harm to an individual as judged by a reasonable person and
- the School has not been able to prevent the potential harm through remedial action.

'Personal information' is information about an identified individual, or an individual who is reasonably identifiable. For example, information pertaining to their identity (driver's licence, Medicare number, passport details), personal status (age, living situation, health, religion, gender etc.) or legal status (financial, marital, relational, parental etc.).

'Unauthorised access' involves revealing personal information by a staff member, contractor, student or other third party who would not normally be permitted access.

'Unauthorised disclosure' involves making personal information available beyond the School.

'Loss' refers to information being accidentally made available beyond the control of the School.

'Serious harm' to an individual may include serious physical, psychological, emotional, financial or reputational harm. The seriousness of the harm is gauged by the number of individuals whose personal information is involved, what information may have been accessed and its sensitivity, by whom and their potential intentions.

A '**reasonable person'** is a School staff member who is properly informed and able to make an assessment of the data breach.

'Remedial action' is that taken by the School to remove or reduce access to the information, such as ensuring information shared accidentally is deleted.

EXAMPLES

- A student obtains a staff member's password leading to unauthorised access.
- A staff member leaves their computer unlocked while they are away, leading to unauthorised access.
- A staff member inadvertently provides their credentials to a malicious third party through an email phishing scheme, leading to unauthorised access.

- Personal information is captured in a document that is shared by email or using cloud storage resulting in unauthorised disclosure.
- A teacher misplaces printed personal information used for reference during an excursion, resulting in information loss.

PROCEDURE FOR RESPONDING TO A DATA BREACH

Contain

As soon as School staff suspect a data breach, even before it is determined whether it is an eligible data breach, the following actions should be taken to contain the breach:

- Notify Education Technology Support staff immediately.
- Notify the relevant Head of Primary or Senior School or appropriate Director immediately given the potential serious consequences of the involvement of students and staff.
- Change the network password of individuals whose information may have been lost, without their consent or involvement if necessary.
- Change the system access passwords of any systems that may have been compromised.
- Lock the account of any staff member or student suspected of unauthorised access.
- Capture logs of recent activity of involved staff and students for potential assessment. Assess.

If School staff suspect there has been any data breach, they must quickly (within 30 days, but as soon as possible) assess the following:

- What personal information may have been accessed
- How many individuals were affected
- Who has gained access to the information and their potential
- How long the information has been available
- The seriousness of the potential harm to individuals and ultimately
- Whether the breach is an eligible data breach requiring further action

At any time, the School may attempt remedial action if it could reduce the seriousness of harm.

Notify

When a breach is determined to be an eligible data breach, a response should be planned by the following people:

- The Head of Information Technology to describe the scale and seriousness of harm
- The Head of School, Head of Primary or Senior School to determine disciplinary action and parental involvement where students are involved
- The Directors, Human Resources Manager and Departmental manager where staff members are suspected to have been involved in unauthorised access
- The Chief Financial Officer where there is potential financial loss to the School as a result of the breach
- Police where there is potential physical or criminal risk

Notification needs to be sent to all affected individuals. Should there be widespread data loss affecting people who cannot be specifically identified, the notification may need to be sent to all individuals or made publicly.

A report of any eligible data breach must be sent to the Australian Information Commissioner through the Notifiable Data Breach statement Form.

The notification to affected individuals and the Commissioner must include the following information:

- The identity and contact details of the School
- A description of the data breach
- The kinds of information concerned
- Recommended steps individuals should take in response to the data breach

Review

Following notification, the following actions may be taken:

- Enact plans to prevent similar future data breaches
- Conduct audits to ensure preventative measures are working
- Consider changes to staff and student policies
- Revise staff training
- Update this Data Breach Policy

Appendix 10 - Management of Personal Information Checklist

The Privacy Policy of Mueller College must contain the following information:

Item	School Response
1. The kinds of personal information that the College collects and holds	Refer Table 1 (above)
2. How the College collects and holds personal information	Refer Table 1 (above)
3. The purposes for which the College collects, holds, uses and discloses personal information	Refer Table 1 (above) Refer Collection Notice/Privacy Policy section
4. How an individual may access personal information about the individual that is held by the College and seek the correction of such information	By writing to the Head of College (refer Privacy Policy section 13)
5. How an individual may complain about a breach of the Australian Privacy Principles and how the College will deal with such a complaint	Contact Head of College (refer Privacy Policy section 13)
6. Whether the College is likely to disclose personal information to overseas recipients	May include overseas 'cloud' storage. Refer Collection Notice
7. If the College is likely to disclose personal information to overseas recipients - the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy	USA - eg Google Docs; Edmondo;
8. What happens to unsolicited personal information that is received; also when individuals are no longer associated with Mueller College	Personal information to be de-identified or destroyed - noting the exception relating to employee records