

## Privacy Impact Assessment and School Action Plan

Google Apps for Education

### School Representative:

For the purpose of this policy, your School will be represented by:

School Principal \_\_\_\_\_

School \_\_\_\_\_

- Acknowledge that I have read the *Guidelines for the use of Department brokered cloud services*.
- Acknowledge the school's responsibilities outlined in the guidelines.
- Confirm that this Privacy Impact Assessment has been customised for my school.
- Confirm that my school has assigned staff to required roles.
- Approve for my school to participate in the following online services.
- Acknowledge Google Apps for Education is a cloud system hosted by Google outside of Australia.
- Acknowledge minimal levels of personal information are collected to facilitate system use.
- Acknowledge information is gathered to enable users to log onto systems and is only for school use.

Principal's signature: \_\_\_\_\_

Date: \_\_\_\_\_

*Executive Summary*

Executive Summary

**Context**

Schools continue to adopt and use a range of information and communications technology (ICT) to improve learning and teaching at an accelerated rate.

The number of computers in Victorian government schools has more than doubled over the past five years, having grown to a fleet of over 550,000 devices. Secondary schools have reached a 1-to-1 computer to student ratio, with Primary schools closely following.

**Key Issues**

Schools are implementing co-contribution and bring your own device (BYOD) programs to sustain personalised access to technology.

The introduction of co-contribution and BYOD programs in schools to date has highlighted a number of procurement, technical and operational challenges that cannot be fully addressed using traditional models.

Schools are realising these challenges cannot be fully addressed using traditional models (for example, school file servers are not easily accessed from iOS or Android devices), and are actively turning to cloud based offerings to bridge the gap.

**Actions taken**

The Department plan to provide cloud based capabilities for school use through Google Apps for Education, a suite of cloud based offerings by Google, hosted and supported within, and outside of Australia.

Background

*Background*

**Context**

The introduction of co-contribution and BYOD programs at school level adds a new dimension of procurement, technical and operational challenges as staff and students expect to:

- Access software on a variety of ICT devices; including: PC, Mac, iOS, Android.
- Create, edit, store and retrieve school work on a variety of ICT devices.
- Use more than one ICT device at a time.
- Access software, and their school work from home – regardless of whether they are using the device they bring to school.

Key **risks** associated with individual school adoption and use of cloud services include:

- Schools may **not** fully evaluate the risks and associated privacy impact associated with each individual cloud service they intend to use.
- Schools may **not** have the necessary skills to implement privacy, data protection and cyber-safety measures for each cloud service they intend to use.
- As all cloud services are different, individual school configuration of privacy, data protection and cyber safety controls for disparate cloud services provides the potential for **inconsistency** and **unmitigated risk**.
- Individual school adoption results in a **time commitment** for each school to implement, manage and maintain each cloud service. This is inefficient and costly to schools when compared to a Department brokered cloud service.

Google Apps

*Google Apps for Education*

Google Apps for Education is a cloud-based offering by Google, hosted and supported within, and outside of Australia, providing access to:

- Google Docs software (PC, Mac, iOS, Android)
- Online storage (Google Drive)
- Web and social collaboration (Classroom, Sites and Calendar)
- Email (Gmail)
- Instant messaging and desktop conferencing (Hangouts)

Organisations can choose to implement some, or all of the above features of Google Apps for Education at an organisational level, and at a per-user level.

For example:

- The Department could choose to make available access to the Google Docs and online storage (Google Drive) features only.
- From the features made-available by the Department, individual users could opt-in or opt-out of using these features.

For more information on the Google offering refer to: <https://www.google.com/edu/products/productivity-tools/>

## Privacy Impact Assessment

### Introduction and Section 1

The purpose of the Privacy Impact Self Assessment is to assist your school assess its privacy risk exposure and mitigating controls required to comply with the Privacy Data and Protection Act 2014 (PDPA) and provide a safe environment for the use of Google Apps for Education.

**NOTE: Google Apps for Education is a cloud system hosted by Google for educational purposes only. Minimal levels of personal information are to be collected by schools. Information is gathered to enable users to log onto systems and is only for school use. This information is hosted by Google.**

#### Information shared with Google

1 Name

2 Username

3 Any information the user chooses to share with Google Apps for Education

### Section 1 - Select the services you intend to use

Google Apps for Education Applications	Deployed by your school?
<b>Standard Applications</b>	
<i>Classroom</i>	Yes
<i>Gmail</i>	Yes
<i>Drive</i>	Yes
<i>Calendar</i>	Yes
<i>Docs, Sheets, Slides</i>	Yes
<i>Sites</i>	Yes
<i>Hangouts</i>	Yes
<i>Vault</i>	Yes

### Section 2 - Complete the privacy questionnaire to suit your school

Please review and update questions in Section 2 (Part 1 to Part 8) by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Risks and questions listed in this assessment were developed from Australian Privacy Principles ("APP") and Victorian Information Privacy Principles ("IPP").

### Section 3 - Implement the action plan

Based on the answers you have provided from Section 2 (Part 1 to Part 8), there may be areas where your school needs to improve on to ensure that information privacy of students using Google Apps for Education is appropriately protected.

For each of the actions required, please provide the name of your staff who will be responsible for the action and target date. This listing can also be used as an action tracker to ensure that all actions have been considered and completed.

### Section 4 - Assign staff to required roles

Please assign staff to required roles as described in the ICT Online Services Policy, including School Online Services Coordinator(s), School Identity Administrator(s), School Welfare Officer(s) and Specialist Technician.

### Section 5 - Note the Privacy analysis conducted by the Department for the use of Google Apps

Please note the Privacy analysis conducted by the Department for the use of Google Apps.

1

Select

2

Complete

3

Implement

4

Assign

5

Note

Section 2 - Complete the privacy questionnaire to suit your school



Part 1 - Personal and Sensitive Information

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

**Q1.1** What personal information of staff and students may be captured using Google Apps for Education?

**Q1.2** What sensitive information of staff and students may be captured using Google Apps for Education?

**Q1.3** Will there be use of unique or government identifiers?

**Q1.4** Will students be allowed to be anonymous?

Please Select	Comments (if any)
Name, username, birthdate, job title	<p><i>Students and their family's personal information may be captured as part of your child utilising online services in the classroom.</i></p> <p><i>Personal information is information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act applies.</i></p>
None	<p><i>The policy will be that no sensitive information is to be captured as Google Apps for Education is meant to be used for classroom activity. However there may be the risk that students store documents with sensitive information on the cloud.</i></p>
Yes	<p><i>Yes, Google Apps for Education will use their IDAM or User name, it will be a Department generated one, not one specific for Google Apps for Education.</i></p>
No	<p><i>From an educational and duty of care perspective, students need to be identifiable when using DET ICT services. Use of Google Apps for Education is no different in this regard.</i></p> <p><i>Secure system that needs to login to so cannot be anonymous.</i></p>

**Privacy Impact Assessment**

*Section 2 - Complete the privacy questionnaire to suit your school*

**2**  
Complete

**Part 2 - Collection of Information**

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP 1, APP 3 and APP 5	While Google Apps for Education is used for classroom purposes, there is a risk that students and teachers may collect information and store it on Google Apps for Education for non-school purposes.	Possible	Minor	Medium
IPP1, IPP10, APP 3 and APP 4	While Google Apps for Education is used for classroom purposes, there is a risk that sensitive information is collected and stored in the cloud without consent.	Unlikely	Moderate	Medium

**Considerations for your school to implement prior to deployment of Google Apps for Education**

		Please Select	Comments (if any)
Q2.1	Will your school have an Acceptable Use Agreement? Will it contain segments stating that Google Apps for Education is only to be used for school related purposes?	Yes	By selecting Yes, the School confirms that it has an Acceptable Use Agreement in place prior to deployment of Google Apps for Education. This Agreement outlines that the use of Google Apps for Education is limited to school related activities.  (Refer to 2.3 of Guidelines for Department Brokered ICT Online Services)
Q2.2	Will your school inform students about the Acceptable Use of ICT and what their parents/guardians have agreed to in the Acceptable Use Agreement?	Yes	By selecting Yes, the School confirms that it will inform students of the Acceptable Use of ICT prior to deployment of Google Apps for Education. As part of this, they will be educated on the terms their parents/guardians have agreed to in the Acceptable Use Agreement.  (Refer Attachment 4 of Guidelines for Department Brokered ICT Online Services)
Q2.3	Will there be methods for school staff to monitor students' use of Google Apps for Education to determine if student's information is collected without their consent, and notify them and/or their parents?	Yes	Only students whose parents/guardians have provided consent forms will be provided access to Google Apps for Education. On an ongoing basis, staff will supervise the use of Google Apps for Education.  (Refer to Attachment 3(e) of the Guidelines for Department Brokered ICT Online Services)
Q2.4	Will your School Online Services Coordinator(s) and Specialist Technician be provided with sufficient time to access and retrieve all content, where necessary from the Google Apps for Education applications?	Yes	By selecting Yes, the School confirms that the School Online Services Coordinator and Specialist Technician will be granted access to retrieve contents from Google Apps for Education where required. This will be implemented prior to deployment of Google Apps for Education.  (Refer to Attachment 3(a),(d) of the Guidelines for Department Brokered ICT Online Services)

**Prior to using the cloud service schools must obtain fully informed, freely given, current and specific consent from an individual (or their parent, guardian or carer in the case of a student) in order to address duty of care, privacy and copyright legal issues.**

**Please go to Part 3.**

Privacy Impact Assessment

Section 2 - Complete the privacy questionnaire to suit your school



Part 2 - Collection of Information

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP 1, APP 3 and APP 5	While Google Apps for Education is used for classroom purposes, there is a risk that students and teachers may collect information and store it on Google Apps for Education for non-school purposes.	Possible	Minor	Medium
IPP1, IPP10, APP 3 and APP 4	While Google Apps for Education is used for classroom purposes, there is a risk that sensitive information is collected and stored in the cloud without consent.	Unlikely	Moderate	Medium

Considerations for your school to implement prior to deployment of Google Apps for Education

Please Select	Comments (if any)
---------------	-------------------

**Privacy Impact Assessment**  
**Section 2 - Complete the privacy questionnaire to suit your school**

**2**  
Complete

**Part 3 - Privacy Policy**

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP 5 IPP 9	Insufficient information in the school Privacy Policy resulting in parents / students not being aware of how privacy is managed by schools.	Possible	Minor	Medium
APP 1 APP 8	Students and parents / guardians do not have access to information about school's information handling practices and / or the school privacy handling practice is out dated.	Possible	Minor	Medium

The Department has published several policies for the use of ICT resources and online services. **Acceptable Use Policy**  
<http://www.education.vic.gov.au/school/principals/infrastructure/pages/acceptableuse.aspx>

**Information Privacy**  
<http://www.education.vic.gov.au/school/principals/spag/governance/Pages/privacy.aspx>

**Privacy Complaints Handling Policy**  
<https://edugate.eduweb.vic.gov.au/Services/privacy/Privacy%20Documents/DEECD%20information%20privacy%20complaints%20handling%20policy.doc>

Google publishes its online terms and conditions for Google Apps for Education. **\*Google Apps for Education Agreement July 2015**  
[http://www.google.com/apps/intl/en-in/terms/education\\_terms.html](http://www.google.com/apps/intl/en-in/terms/education_terms.html)  
**\*\*Data Processing Amendment to Google Apps Agreement**  
[https://www.google.com/intx/en/work/apps/terms/dpa\\_terms.html](https://www.google.com/intx/en/work/apps/terms/dpa_terms.html)

**Considerations for your school to implement prior to deployment of Google Apps for Education**

**Please Answer / Select                      Comments (if any)**

**Q3.1**      In addition to Department policies, what school policies will apply to the use of the online service?

Bullying and Harrassment Policy, Child Safety Policy, ICT Acceptable Use Policy, Safe Guarding Children and Young People Code of Conduct

**Q2.1**      Does your school have a Privacy Policy?

<b>Yes</b>	From 2018, the Department of Education and Training has a Schools' Privacy Policy that applies to all schools: <a href="http://www.education.vic.gov.au/Pages/schoolsprivacypolicy.aspx">http://www.education.vic.gov.au/Pages/schoolsprivacypolicy.aspx</a>
------------	---

**Q3.2**      Will your school Privacy Policy address the following:  
**(a)** the type of personal information that your school collects and holds;  
**(b)** how your school collects and holds personal information;  
**(c)** the purposes for which your school collects, holds, uses and discloses personal information;  
**(d)** how students / parents may access their personal information and if needed, correct such information;  
**(e)** how students / parents should report a breach of their Privacy, and the school's process for dealing with reported breaches of Privacy;  
**(f)** your school's policy on disclosing personal information to overseas recipients;  
  
**(g)** where your school's policy is to report personal information to overseas recipients, the countries that personal information may be disclosed to.

<b>Yes</b>	

**Q3.3**      Will parents be able to obtain a copy of your Privacy Policy easily and free of charge?

<b>Yes</b>	
------------	--

**Privacy Impact Assessment**  
**Section 2 - Complete the privacy questionnaire to suit your school**

**2**  
Complete

**Part 3 - Privacy Policy**

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP 5 IPP 9	Insufficient information in the school Privacy Policy resulting in parents / students not being aware of how privacy is managed by schools.	Possible	Minor	Medium
APP 1 APP 8	Students and parents / guardians do not have access to information about school's information handling practices and / or the school privacy handling practice is out dated.	Possible	Minor	Medium

The Department has published several policies for the use of ICT resources and online services. **Acceptable Use Policy**  
<http://www.education.vic.gov.au/school/principals/infrastructure/pages/acceptableuse.aspx>

**Information Privacy**  
<http://www.education.vic.gov.au/school/principals/spag/governance/Pages/privacy.aspx>

**Privacy Complaints Handling Policy**  
<https://edugate.eduweb.vic.gov.au/Services/privacy/Privacy%20Documents/DEECD%20information%20privacy%20complaints%20handling%20policy.doc>

Google publishes its online terms and conditions for Google Apps for Education.  
**\*Google Apps for Education Agreement July 2015**  
[http://www.google.com/apps/intl/en-in/terms/education\\_terms.html](http://www.google.com/apps/intl/en-in/terms/education_terms.html)  
**\*\*Data Processing Amendment to Google Apps Agreement**  
[https://www.google.com/intx/en/work/apps/terms/dpa\\_terms.html](https://www.google.com/intx/en/work/apps/terms/dpa_terms.html)

Considerations for your school to implement prior to deployment of Google Apps for Education

Please Answer / Select	Comments (if any)
Yes	

**Q3.4** Will the school's privacy policies and procedures be reviewed at least annually?

Please go to Part 4.

**Privacy Impact Assessment**

*Section 2 - Complete the privacy questionnaire to suit your school*

**Section 4 - Use of Information**



Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP2 APP 6 APP 7	Google Apps for Education will primarily be used for classroom activities. Except where is required by law, there is a risk that a student's personal and/or sensitive information is inadvertently <b>used</b> for non-school purposes or without parental/guardian consent.	<b>Unlikely</b>	<b>Moderate</b>	<b>Medium</b>

**Considerations for your school to implement prior to deployment of Google Apps for Education**

**Please Answer / Select**

**Comments (if any)**

**Q4.1** How will your school **use** the information collected on staff and students?

*The School will use personal information for teaching and learning activities only. (Refer Attachment 1 of Guidelines for Department Brokered ICT Online Services)*

**Q4.2** Will your School Identity Administrator be able to remove individual Google Apps for Education access authority in a timely manner when access is no longer needed?

**Yes**

*Once the School revokes access removal will be processed by Google. No more than 180 days after expiration or termination of Customer's use of an Online Service, Google will disable the account and delete Customer Data from the account*

*(Refer Google Apps for Education factsheet in Guidelines for Department Brokered ICT Online Services and Section 7 - Data Correction, Blocking and Deletion, of the Data Processing Amendment to Google Apps Agreement\*\*)*

**Q4.3** In the event sensitive information is collected, how will your school ensure it is not used and stored in Google Apps for Education?

*All staff will be informed that you must not place personal, sensitive, health or security classified information into your Vault*

*In addition, the terms and conditions of Google state that customer data will not be used for purposes other than for the provision of online services. Google will not sell user data to third parties or use it for non-school related purposes.*

Only the Department can access Google Apps for Education audit logs and student data trails. If your school requires access, please obtain written approval from your School Principal and submit a request to the Department.

\*Google Apps for Education Agreement, July 2015  
[http://www.google.com/apps/intl/en-in/terms/education\\_terms.html](http://www.google.com/apps/intl/en-in/terms/education_terms.html)

\*\*Data Processing Amendment to Google Apps Agreement, July 2015  
[https://www.google.com/intx/en/work/apps/terms/dpa\\_terms.html](https://www.google.com/intx/en/work/apps/terms/dpa_terms.html)

**Please go to Part 5.**

**Privacy Impact Assessment**

*Section 2 - Complete the privacy questionnaire to suit your school*

**Part 5 - Access and Disclosure**

**2**  
Complete

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP 2 APP 6 APP 7 APP 12	Google Apps for Education will primarily be used for classroom activities. Except where required by law, there is a risk that students' personal and sensitive information may be disclosed for non-school purposes or without parental/guardian consent.	Unlikely	Moderate	Medium
IPP6	While an individual has a right to access their personal and sensitive information, there is a risk that it is not provided in accordance with the <i>request for information about students</i> guidance.	Unlikely	Moderate	Medium
IPP7	The risk that student's personal and sensitive information is used for direct marketing purposes	Rare	Major	Medium

**Considerations for your school to implement prior to deployment of Google Apps for Education**

		Please Select	Comments (if any)
Q5.1	Will your school staff be aware of the policy in dealing with <i>requests for information about students</i> ? <a href="http://www.education.vic.gov.au/school/principals/spag/safety/Pages/requestinfo.aspx">http://www.education.vic.gov.au/school/principals/spag/safety/Pages/requestinfo.aspx</a>	Yes	<i>By selecting yes, the School confirms that its staff will be informed of policy for dealing with information requests.</i>  <i>(Refer to Attachment 3(a) of the Guidelines for Department Brokered ICT Online Services)</i>
Q5.2	Have you answered <b>Yes</b> to question 2.1 and 2.4 with regards to having an Acceptable Use Agreement and informing students and staff of Privacy and Acceptable use of ICT?	Yes	<i>As indicated in 2.1-2.4, the School has confirmed that it has an Acceptable Use Agreement, will inform staff and students on Privacy and Acceptable Use of ICT, and has the ability to retrieve information.</i>
Q5.3	If you have answered <b>Yes</b> to 5.2, does your school's Acceptable Use policy and procedures address not <b>disclosing</b> personal and sensitive information for non-school purposes or without parental/guardian consent?	No	<i>Please refer to the Action items for Section 2.1-2.4, that require implementation prior to deployment of Google Apps for Education.</i>
Q5.4	The terms and conditions of Google state that customer data will not be used or disclosed for purposes other than providing the online services. Information will not be used for direct marketing purposes. (Refer to Section 5.3 - Processing Restrictions, Data Processing Amendment to Google Apps Agreement**)  If, on advice from the Department, that Google has changed their terms and conditions, will your school have procedures in place to inform students/parents if the following occur:  <b>(a)</b> Information is <b>used or disclosed</b> by your school for purposes other than those with parental consent, this may include research or law enforcement; or	Yes	<i>By selecting Yes, the School confirms that it will have procedures in place to inform students/parents that information is used or disclosed for purposes other than those with parental consent, including research or law enforcement.</i>

**Privacy Impact Assessment**

*Section 2 - Complete the privacy questionnaire to suit your school*

**Part 5 - Access and Disclosure**

**2**  
Complete

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP 2 APP 6 APP 7 APP 12	Google Apps for Education will primarily be used for classroom activities. Except where required by law, there is a risk that students' personal and sensitive information may be disclosed for non-school purposes or without parental/guardian consent.	Unlikely	Moderate	Medium
IPP6	While an individual has a right to access their personal and sensitive information, there is a risk that it is not provided in accordance with the <i>request for information about students</i> guidance.	Unlikely	Moderate	Medium
IPP7	The risk that student's personal and sensitive information is used for direct marketing purposes	Rare	Major	Medium

**Considerations for your school to implement prior to deployment of Google Apps for Education**

(b) Notices are received from the Department or Google that information has been/will be used or disclosed for secondary or other unexpected purposes.

**Please Select**

**Comments (if any)**

Yes	<i>By selecting Yes, the School confirms that it will have procedures in place to inform students/parents when notices are received from the Department or Google that information has been/will be used or disclosed for secondary or other unexpected purposes.</i>
-----	---

\*Google Apps for Education Agreement, July 2015

[http://www.google.com/apps/nll/en-in/terms/education\\_terms.html](http://www.google.com/apps/nll/en-in/terms/education_terms.html)

\*\*Data Processing Amendment to Google Apps Agreement, July 2015

[https://www.google.com/intl/en/work/apps/terms/dpa\\_terms.html](https://www.google.com/intl/en/work/apps/terms/dpa_terms.html)

**Based on your selections above, please take the following actions:**

• Ensure your school's Acceptable use policy, agreement and Privacy policy addresses not disclosing personal and sensitive information for non-school purposes or without parental/guardian consent.

## Privacy Impact Assessment

### Section 2 - Complete the privacy questionnaire to suit your school

#### Part 6 - Monitor

2 Complete

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP 3 APP 10	Inappropriate content is shared among students from Google Apps for Education shared sites, documents or other facilities.	Unlikely	Moderate	Medium
IPP 6 APP 1 APP 12 APP 13	Enquiries, changes or complaints raised to schools when students using Google Apps for Education are not appropriately addressed or escalated.	Possible	Moderate	Medium

#### Considerations for your school to implement prior to deployment of Google Apps for Education

Please Select

Comments (if any)

**Q6.1** Will your school have procedures in place for:

**(a)** performing annual reviews of student consent against actual access?

**(b)** performing annual reviews of content stored on Google Apps for Education for appropriate use?

**Q6.2** Will students, teachers or school staff be aware of how to report, manage and escalate issues/abuses when using online services?

<b>Yes</b>	<p><i>By selecting Yes, the School confirms that annually, it will review its access against the consents received.</i></p> <p><i>(Refer to Attachment 4 of Guidelines for Department Brokered ICT Online Services)</i></p>
<b>Yes</b>	<p><i>By selecting Yes, the School confirms that it will perform annual reviews of content stored on Google Apps for Education for appropriate use.</i></p>
<b>Yes</b>	<p><i>By selecting Yes, the School confirms that it will have a process for, and inform students, teachers or school staff to report, manage and escalate issues/abuses when using online services.</i></p> <p><i>(Refer to 8.4 of the Guidelines for Department Brokered ICT Online Services).</i></p>

**Teachers and other school staff have a responsibility to take reasonable steps to protect students from risks of injury, including those that may be encountered within the online learning environment.**

**Privacy Impact Assessment**

*Section 2 - Complete the privacy questionnaire to suit your school*

**Part 7 - Information Security**

**2**  
Customise

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence	Inherent risk rating
IPP 4 APP 11	A number of the compliance controls refer to the Google Services Terms and Conditions. There is a risk that Google may reduce compliance controls within their terms and conditions, resulting in privacy risk exposure to the Department.	Possible	Moderate	Medium
IPP 4 APP 11	Whilst Google, the Department and schools have controls and procedures in place to protect information security, information about students may be misused, lost or accessed, modified or disclosed inappropriately. This risk is not isolated to the use of cloud systems, however can be exacerbated by their use.	Rare	Moderate	Low
IPP 4 APP 11	Staff are not given appropriate levels of training on Google Apps for Education resulting in lack of skills to effectively monitor the Google Apps for Education environment and promote appropriate privacy practices.	Possible	Moderate	Medium
IPP 8 IPP 9	With respect to trans-border data flows, the risk that personal and sensitive information is transferred to someone or an organisation outside Victoria, without parent/guardian consent, for purposes other than the performance of a contract, and that the service provider is not subject to upholding Information Privacy Principles.	Likely	Minor	Medium

**Considerations for your school to implement prior to deployment of Google Apps for Education**

While Google Apps for Education Terms & Conditions provides that Google works continuously to meet rigorous privacy and compliance standards as evidenced by undergoing regular independent audits of its infrastructure, applications and operations (Refer Google Apps for Education Agreement\* and Data Processing Amendment to Google Apps Agreement\*\*);

Will there be the following additional controls in place:

- Q7.1** Will there be a process for monitoring Google's compliance with their privacy and compliance standards, and monitor changes to terms and conditions?
- Q7.2** Will parents/guardian's consent be sought for approval of information being disclosed to organisations outside Victoria?

**Please Select**

**Comments (if any)**

<b>Yes</b>	<i>The Department will be monitoring the service provider and reviewing their services periodically. (Refer to Section 6 of the Guidelines for Department Brokered ICT Online Services).</i>
<b>Yes</b>	<i>The Consent Form template notifies parents of information stored within and outside Australia. (Refer to Google School Information Pack).</i>



## Privacy Impact Assessment

### Section 2 - Complete the privacy questionnaire to suit your school

#### Part 8 - Destroy

2

Complete

Please review and update questions below by either selecting answers from the dropdown list or providing additional comments in cells highlighted in yellow.

Reference to privacy principles	Potential risks	Likelihood of occurrence	Impact of occurrence
IPP 4 APP 11	Students' information remains on Google Apps for Education when they leave a school or the Victorian school system.	<b>Possible</b>	<b>Moderate</b>

**Considerations for your school to implement prior to deployment of Google Apps for Education**

**Please Select**

**Comments**

**Q8.1** As part of your annual review process, will your School Online Services Coordinator(s) be able to destroy / delete students information / records stored online when students leave your school or the Victorian school system?

**Yes**

*By selecting Yes, the School Online Services Coordinator(s) will be able to delete student information.*

*Once the School revokes access to Google Apps for Education, all data processed by Google. No data is retained after expiration or termination of an Online Service, Google account and delete Customer account.*

*(Refer Google Apps for Education Guidelines for Department of Education Services and Section 7 - Blocking and Deletion, or Amendment to Google Apps for Education)*

**Please check if you have updated all the questions from Part 1 to Part 8 and proceed to Section 3: Implement the action plan.**



**Inherent risk rating**

**Medium**

**ts (if any)**

*ool confirms that its  
ordinator(s) will be  
ormation as required.*

*s access removal will be  
o more than 180 days  
ation of Customer's use  
ogle will disable the  
omer Data from the*

*ducation factsheet in  
nt Brokered ICT Online  
Data Correction,  
f the Data Processing  
pps Agreement\*)*



## Privacy Impact Assessment

### Section 3 - Implement the action plan

[Click Here](#)

to update the action listing for your school.

3

Implement

Based on your answers to the questionnaire, your school needs to implement the following actions to ensure that information privacy of students using Google Apps for Education is appropriately protected.

For each of the actions required, please provide the name of your staff who will be responsible for the action and target date. This listing can also be used as an action tracker to ensure that all actions have been considered and completed.

Actions to be taken	Responsibilities	Target Date	Status
• Ensure your school's Acceptable use policy, agreement and Privacy policy addresses not disclosing personal and sensitive information for non-school purposes or without parental/guardian consent.	Jayden Spudvilas-Powell	31/7/18	<b>In progress</b>

## Privacy Impact Assessment

### Section 4 - Assign staff to required roles

# 4

Assign

Please assign staff to required roles as described in the ICT Online Services Policy, including School Online Services Coordinator(s), School Identity Administrator(s), School Welfare Officer(s) and Specialist Technician.

School:

0

Position	Name	Email	Telephone
School Online Services Coordinator	Jayden Spudvilas-Powell	<a href="mailto:spudvilas-powell.jayden.l@edumail.vic.gov.au">spudvilas-powell.jayden.l@edumail.vic.gov.au</a>	9743 5818
School Online Services Coordinator			
School Identity Administrator	Michelle Costa	<a href="mailto:costa.michelle.m@edumail.vic.gov.au">costa.michelle.m@edumail.vic.gov.au</a>	9743 5818
School Identity Administrator			
School Welfare Officer	Margaret Campbell	<a href="mailto:campbell.margaret.r@edumail.vic.gov.au">campbell.margaret.r@edumail.vic.gov.au</a>	9743 5818
School Welfare Officer			
Specialist Technician	Waqas Iftikhar	<a href="mailto:iftikhar.waqas.w@edumail.vic.gov.au">iftikhar.waqas.w@edumail.vic.gov.au</a>	9743 5818
Specialist Technician			

5  
Note

## Compliance summary

No.	IPP	Compliance criteria	Assessment
1	1.1	<i>Collection</i> - Is all the information collected NECESSARY for the program?	Yes
2	8.1	<i>Collection</i> - Is it lawful or practicable for the individual to remain anonymous for the purpose of the program?	No
3	1.3	<i>Notice</i> - Have you taken reasonable steps to ensure that the individual whose information is collected is made aware of the information below? <ul style="list-style-type: none"> <li>• The fact that the individual can access their information</li> <li>• The purpose for the collection</li> <li>• To whom the organisation will disclose the information</li> <li>• Any law requiring the information to be collected</li> <li>• Consequences, if any, to the individual if the information is not provided</li> </ul>	Yes
4	1.4 1.5	<i>Direct/indirect collection</i> - Is the information being collected DIRECTLY from the individual?	Partial
5	7.1 7.2 7.4	<i>Unique identifier</i> - Will this program assign or collect a unique identifier?	No
6	10.1 (a-d)	<i>Sensitive information</i> - Will this program collect sensitive information?	No
7	10.2 (a-d)	<i>Sensitive information</i> - Will the sensitive information be used for a research purpose?	N/A

No.	IPP	Compliance criteria	Assessment
8	2.1	<i>Use and disclosure</i> - Information will ONLY be used or disclosed for the primary purpose identified in this PIA.	Yes
9	2.1 (a-h) 2.2	<i>Use and disclosure</i> - In addition to using and disclosing information for the primary purpose it was collected, personal information will be used or disclosed for a secondary purpose.	N/A
10 (a)	7.2	<i>Use and disclosure of a unique identifier assigned by another organisation</i> – Will this program use or disclose a unique identifier assigned to an individual by another organisation?	Yes
10 (b)	7.3 (a-c)	<p><i>Use and disclosure of a unique identifier assigned by another organisation</i> – Will this program use or disclose a unique identifier assigned to an individual by another organisation?</p> <p>Use and disclosure of a unique identifier assigned by another organisation – The unique identifier assigned to an individual by another organisation will not be used or disclosed unless one of the following apply:</p> <ul style="list-style-type: none"> <li>• It is necessary for the organisation to fulfil its obligation to the other organisation</li> <li>• The individual has consented</li> <li>• One or more of the following apply: (see IPP 2.1 (d)-(g) for full conditions) <ul style="list-style-type: none"> <li>o A serious threat to individual or public health, safety or welfare</li> <li>o Reporting a suspected unlawful activity to the relevant person or authority as part of an investigation</li> <li>o It is required or authorised by law</li> <li>o The organisation reasonably believes the use or disclosure is reasonably necessary by or on behalf of a law enforcement agency (see IPP 2.1 (g) for full description)</li> </ul> </li> </ul>	Noted (See comments)
11 (a)	9.1	<i>Transborder data flows</i> – The initiative will transfer personal information to an organisation or person outside of Victoria (other than the organisation or the individual)	Yes

No.	IPP	Compliance criteria	Assessment
11 (b)	9.1 (a-f)	<p><i>Transborder data flows</i> – Personal information will only be transferred to someone outside of Victoria (other than the organisation or the individual) if one of the following apply:</p> <ul style="list-style-type: none"> <li>• The organisation reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the IPPs</li> <li>• The individual consents to the transfer</li> <li>• The transfer is necessary for the performance of a contract between the individual and the organisation</li> <li>• The transfer is necessary as part of a contract in the interest of the individual between the organisation and a third party</li> <li>• All of the following apply: <ul style="list-style-type: none"> <li>o The transfer is for the benefit of the individual; AND</li> <li>o It is impractical to obtain consent; AND</li> <li>o If it were practicable the individual would likely consent.</li> </ul> </li> <li>• The organisation has taken reasonable steps so that the information transferred will be held, used and disclosed consistently with the IPPs.</li> </ul>	Noted (See comments)
12	3.1	<p><i>Data quality</i> – Describe steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date.</p>	
13 (a)	4.1 and VPDSF	<p><i>Data security</i> - The program has taken reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.</p>	Yes
13 (b)	4.2	<p><i>Records management</i> - The initiative will take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purpose.</p>	Yes
14 (a)	5.1	<p><i>Openness</i> – The organisation has a document available for public review that sets out the policies for the management of personal information.</p>	Yes
14 (b)	5.2	<p><i>Openness</i> - The organisation has steps in place to allow an individual to know what personal information it holds about them and for what purposes it collects, uses and discloses it.</p>	Yes

No.	IPP	Compliance criteria	Assessment
15	6	<p><i>Access and correction</i> - The Access and Correction principle (IPP 6) entitles individuals to view and obtain copies of their personal information and to correct personal information held about them. IPP 6 is designed to supplement existing access and correction rights under the Freedom of Information Act 1982 (FOI Act). Information held by a Victorian public sector organisation is subject to the FOI Act and therefore do not need to assess against IPP 6.</p> <p>Where the public sector outsources part of their program services to a CSP, the CSP will be required to comply with IPP 6 but only in relation to the CSP's provision of service under a state contract. Please refer to Outsourcing and Privacy Guidelines for additional information on CSPs and their obligations under IPP 6.</p>	Noted