PRIVACY IMPACT ASSESSMENT

MICROSOFT OFFICE 365

AND

GOOGLE APPS FOR EDUCATION

FOR: EDUCATION AND TRAINING

DIRECTORATE, ACT

19 SEPTEMBER 2014

Table of Contents

1. EXECUTIVE SUMMARY

The Education and Training Directorate, Australian Capital Territory (ETD) has asked Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) on the planned implementations of both the Microsoft Office 365 (O365) and Google Apps for Education (GAFE) offerings.

This implementation is part of ETD's Digital Schools Strategy aimed at providing the digital tools and capabilities in ACT schools that match the transformational change in education and training methods and technologies that has occurred over recent years and to meet teacher and student expectations that have accompanied that transformation.

ETD recognises that implementing cloud based applications such as O365 and GAFE raise potential privacy issues and it is its practice to commission a PIA for each new cloud service.

IIS was asked to provide a report containing advice and/or recommendations on:

- disclosure and visibility of personal information of students and teachers both internally (across schools) and externally to GAFE and O365
- on any privacy, secrecy or other relevant legislation applying to information flow used in GAFE and O365 with reference to the Territory Privacy Principle (TTPs) in the Information Privacy Act 2014 (ACT): in particular:
  - consents to uses and disclosures involved, including best practice
  - managing enhanced collaboration across different schools disclosure between schools, for example, global email addresses.

1.1 FINDINGS AND RECOMMENDATIONS/ADVICE

1.1.1 DISCLOSURE AND VISIBILITY OF PERSONAL INFORMATION OF STUDENTS AND TEACHERS EXTERNALLY

1.1.2 GAFE

IIS finds that the risk of privacy harms to students and teachers through misuse or inappropriate disclosure of personal information collected about students and teachers though use of GAFE is low. GAFE appears to comply with the use and disclosure requirements of TPP 6 in the Information Privacy Act.

Google has reduced the risk relating to advertising through its announcement that it will no longer scan Gmail for advertising purposes within the ETD environment which means it no longer collects through Gmail information that could be used for advertising. It still can compile a significant profile from the search information and browser history of a user but it makes satisfactory statements which limit use and disclosure of such information to appropriate purposes.

The main concern relating to GAFE is its complex privacy framework which makes it difficult to easily gain a picture of the information that Google collects and its approach to privacy and security specifically for GAFE. Furthermore, although public pressure has created an impetus to tighten rather than loosen privacy protections, there appear to be few concrete impediments to Google unilaterally changing its approach to privacy, for example, using information for new purposes, which could be detrimental to the privacy interests of users. This lack of transparency and uncertainty heightens ETD's risk of perceptions of privacy harm that might not be based on fact. IIS

considers that ETD's current approach to informing parents and students about privacy and GAFE is unlikely to meet the notice requirements in TPP 5. A key mechanism for managing residual privacy risks particularly for those who are privacy sensitive is for ETD to provide clear information about the privacy options that they can exercise both within GAFE (of which there are a number) and through browser settings.

Recommendation 1 – Develop a clear statement of Google's approach to privacy in GAFE

Recommendation Accepted by ETD. See page 19 for comments

IIS recommends that ETD works with Google to develop a short but clear and accurate statement covering GAFE as rolled out by ETD that sets out:

- the kinds of information about users that Google collects through use of GAFE (including content, server logs, browsing history, location data and covering core and any additional services that are switched on)
- the purposes for which Google collects, uses and discloses such information
- the purposes for which Google will not use or disclose such information where that will add reassurance and clarity – for example, a statement that Google does not use GAFE information to tailor services when a user is interacting with Google products outside the ETD environment
- the fact that Google uses and discloses aggregate information drawn from logs for trend and other purposes and reassures that this is properly de-identified and cannot be associated with a user's account now or in the future
- GAFE's process and timing for deleting all the types of information about students and teachers it holds when a user become an ex-student or ex-teacher
- a statement (which should create as much certainty as possible) which indicates the extent of ETD and user control should Google decide to change its services or privacy policy in a way that has a detrimental impact on the privacy of ETD GAFE users
- an outline of the steps that ETD takes to assure itself that Google complies with its privacy undertakings outlined in the statement
- include the fact that information is stored offshore
- outline an access, correction and complaints process
- links to where the reader can get more information.

ETD should provide this statement to parents, students and teachers before ETD fully rolls out GAFE and emphasise the importance of reading the document before giving consent.

Recommendation 2 – Information to parents, students and teachers on privacy options

Recommendation Accepted by ETD. See page 19 for comments

IIS recommends that ETD provide information that is easy to access, read and understand about the privacy options available to users both within GAFE or using other mechanisms such as those available through browser settings and use of browser sessions.

1.1.3 O365

IIS finds that there is minimal risk of privacy harms through misuse or inappropriate disclosure of personal information collected about students and teachers by O365. Microsoft Office 365 has a coherent privacy framework which includes options for supplementary contractual provisions and publicly available documentation which state clearly that it only collects information necessary to enable it to provide Microsoft Office 365 services. It rules out scanning, indexing or data mining for advertising purposes. It does not develop a profile on users apart from the information necessary to provide the service and provide a good user experience. Microsoft keeps O365 logically and physically separate from its consumer offerings which do rely on advertising for revenue generation. The risk of function creep is minimal if ETD enters into supplementary contractual terms with Microsoft. EDT's pilot consent form provides clear information about how O365 handles personal information but it requires some minor tweaking to ensure that it meets the notice requirements of TPP 5. It would also help student and teachers if EDT gave them information about options for exercising privacy choice within O365 and within the browser.

Recommendation 3 – Privacy notice

Recommendation Accepted by ETD. See page 36 for comments

IIS recommends that ETD amends its O365 Privacy Information and Consent form to ensure that it complies with the notice requirements outlined in TPP 5. For example, it should include information about access, correction and complaints processes.

Recommendation 4 – Contractual supplement

Recommendation Accepted by ETD. See page 36 for comments

IIS recommends that ETD enter into a contractual supplement similar to the one that Microsoft has developed for customers outside Europe (Office 365 Security Amendment (for customers outside of Europe) [English]) which includes provisions that limit its use and disclosure of the personal information it holds in relation to O365.

Recommendation 5 – Information to parents, students and teachers privacy options

Recommendation Accepted by ETD. See page 37 for comments

IIS recommends that ETD provide information that is easy to access, read and understand about the privacy options available to users both within Microsoft 365 or using other mechanisms such as those available through browser settings.

1.1.4 Disclosure and visibility of personal information of students and teachers internally

IIS provides high level advice only on this area as implementation detail on this is not yet available. IIS notes that use of O365 and GAFE, depending on how they are configured could result in students, teachers, and potentially parents being aware of a whole range of information about each other that was not available before, and which it may not be necessary in all cases for them to have, including:

- the email addresses of everyone in schools in the ETD system
- each other's text, voice or video chat conversations
- each other's documents, presentations, sites or material that teachers post

- comments that people including a teacher has made on a shared document or in another forum where views are shared
- whether a person is online and available to communicate (at any time of day or night)
- each other's appointments or meetings

Access to much of this could also be facilitated through the enhanced search mechanisms that are provided.

IIS provides high level advice about how to minimise the risks that could arise from the potential availability of this additional information, including applying a range of tools that limit access where possible.

1.1.5 Other key issues or risks

IIS also provides some high level advice to ETD on other key areas. These relate to:

- revising its Privacy Policy to take into account use of O365 and GAFE including potentially having a separate policy specially for schools
  Advice Partially Accepted by ETD. See page 32 for comments
- the need to ensure real and informed choice in addition to written consent
  Advice Accepted by ETD. See page 33 for comments
- the ability of ETD to establish that it has complied with the requirements of s 21 of the Information Privacy Act regarding contractual provisions with service providers and the requirements of TPP 8 regarding disclosure off shore.
  Advice Accepted by ETD. See page 35 for comments

2. INTRODUCTION

The Education and Training Directorate, Australian Capital Territory (ETD) has asked Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) on the planned implementations of both the Microsoft Office 365 (O365) and Google Apps for Education (GAFE) offerings.

This implementation is part of ETD's Digital Schools Strategy aimed at providing the digital tools and capabilities in ACT schools that match the transformational change in education and training methods and technologies that has occurred over recent years and to meet teacher and student expectations that have accompanied that transformation.

ETD recognises that implementing cloud based applications such as O365 and GAFE raise potential privacy issues and it is its practice to commission a PIA for each new cloud service.

2.1 LEGAL FRAMEWORK

The *Information Privacy Act 2014* (ACT) regulates how personal information is handled by ACT public sector agencies. This Act includes a set of Territory Privacy Principles (TPPs), which cover the collection, use, storage and disclosure of personal information, and an individual's access to and correction of that information.

The Information Privacy Act commenced on 1 September 2014 and replaces the *Privacy Act 1998* (Cth) as in force on 1 July 1994 (and as modified by the Australian Capital Territory Government Service (Consequential Provisions) Act 1994 (Cth), which previously applied to ACT public sector agencies.

The information Privacy Act provides that where ETD enters into a government contract, the contract must contain appropriate contractual measures to ensure that the contracted service provider does not do an act, or engage in a practice, that breaches a TPP (s 21).

ETD also has a privacy policy which sets out the way it handles personal information.

Other relevant legislation in the ACT includes:

- *Territory Records Act 2002*
- *Health Records (Privacy and Access) Act 1997*
- *Freedom of Information Act 1989.*

IIS has briefly assessed these three pieces of legislation but did not identify at this stage any matters of immediate relevance to this scope of work.

2.2 SCOPE

IIS has been asked to provide a report containing advice and/or recommendations on:

- disclosure and visibility of personal information of students and teachers both internally (across schools) and externally to GAFE and O365

- any privacy, secrecy or other relevant legislation applying to information flow used in GAFE and O365 with reference to the TPPs: in particular:
  - consents to uses and disclosures involved, including best practice
  - managing enhanced collaboration across different schools disclosure between schools, for example, global email addresses.

2.3 METHODOLOGY

IIS undertook the following steps in the project:

- Consulted with ETD on the work plan
- Gathered and read documentation
- Analysed the information against the Territory Privacy Principles and other privacy risks that can arise beyond compliance with the law
- Prepared a draft report for ETD to provide feedback
- Revised and finalised the report.

IIS notes that this report does not constitute legal advice and should not be relied upon as such.

3. DESCRIPTION OF PROJECT

ETD is aiming to increase digital capabilities to allow ETD to provide a collaborative learning environment with flexibility and choice for learners with increased access to learning content using the applications they prefer. A key focus is to provide anytime and anywhere access through a range of proven and appropriate and appropriate devices. ETD will provide support within specified parameters to ensure supportability and availability.

IIS understands that ETD is likely to adopt O365 for the corporate environment including teaching and learning and email. However, ETD will make GAFE, including Gmail, available for optional use.

ETD is currently trialling a working prototype of O365 at four selected high schools and is also doing the same in relation to GAFE. A key issue it will focus on is integrating the school's identity management solution with O365 and GAFE to automatically provision students to ensure that any problems with this will have been resolved by the time ETD rolls them out to all schools. ETD will implement a single sign-on system for access to O365 and GAFE. The information being provisioned from internal identity stores to O365 and or GAFE external/cloud systems is proposed to be:

- First/Last/Full name
- User id/login (e.g. unique student number)
- Email address
- User type, i.e. teacher or student (explicitly or inferred by evaluation of email address)
- School (presently not provided to GAFE or O365)
- Year group (presently not provided to GAFE or O365)

ETD is still working on details about how it will implement the applications, including such matters as which features or capabilities of O365 or GAFE will be switched on, and who will have access to

which features. However, for example, only students over the age of 13 will have access to Google +.

For the pilot the following capabilities are included:

- Corporate Environment
    - Corporate Communication using Microsoft Lync Server – Between Teachers
        - Instant Messaging
        - Presence
        - Video Conferencing
- Cloud Based using O365 for education and GAFE – between Student and Student and Student and Teachers
    - Communication
        - Email
        - Instant Messaging
        - Video Conferencing
    - Collaboration
        - Team Spaces
        - Blogs
        - Forums
        - Comments
        - Links
        - Tagging
        - Sharing
        - Subscriptions
        - Notifications
    - Document Management
        - File Types
        - Versioning
        - Upload
        - View / Modify / Delete
        - MetaData
        - History Revisions
    - Search
        - Basic
        - Advanced
    - Content Management
        - Workflow
        - MetaData
        - Page Templates
        - Permissions
        - Publishing
    - Channels
        - Browser based focus using any device

- Standard SOE environment and impact on existing Microsoft products such as MS Office
- Virtual Learning
  - Digital Portfolio
  - Calendars
- User Management
  - Provisioning and maintenance such as students moving schools
  - Administering students and classrooms.

4. POSSIBLE RISKS

This section outlines in table form some high level possible risks that could arise in relation the proposed use of O365 and GAFE in relation to the TPPs. The following section discusses the key risks that arise from this analysis.

Table 1 - A list of Territory Privacy Principles (TPP) with a separate column of associated possible risks for the proposed use of O365 and GAFE

TPP	Possible risk
TPP 1.2 Procedures for compliance and complaints handling	That ETD does not have practices, procedures or systems in place to ensure it complies with the TPPs or can handle complaints, in relation to O365 or GAFE
TPP 1.3 – 1.4 Privacy policy	That ETD's privacy policy does not adequately explain how personal information involved in student and/or teacher use of O365 or GAFE is managed.
TPP 2 Anonymity and pseudonymity	That students or teachers are not given the options of anonymity or pseudonymity in relation to O365 or GAFE when it would be practical to do so.
TPP 3.1 Necessary collection	That O365 or GAFE collect personal information about students or teachers when it is not necessary for their functions or activities. That students or teachers get access to information about each other that they don't need in order to achieve the objectives of the particular capability or application.
TPP 3.3 Consent to collect sensitive information	That O365 or GAFE collect sensitive personal information about students or teachers without their consent.
TPP 3.5 Fair collection	That O365 and/or GAFE collect information about students or teachers that they don't expect to be collected and would not agree to.
TPP 3.6 Direct collection	That O365 or GAFE collect information about students or teachers indirectly without their consent or when it would be reasonable or practicable to collect it directly

TPP	Possible risk
TPP 4 Dealing with unsolicited information	That O365 or GAFE keep unsolicited personal information from students or teachers when the TPPs would not allow it to.
TPP 5 Notice	That students and teachers do not receive adequate information about how O365 or GAFE handles personal about them.
TPP 6 Use and disclosure	That O365 and/or GAFE in their BAU operations use or disclose personal information about students or teachers for purposes that they or students' parents would not reasonably expect or agree to. That Microsoft or Google sometime in the future change their commitments about how they will use or disclose personal information about students or teachers. That information about students or teachers is disclosed to other students or teachers, through use of O365 or GAFE capabilities or applications, that they would not expect or agree to.
TPP 8 Cross-border disclosure	That personal information about students or teachers is transferred overseas to Microsoft or Google without taking reasonable steps to ensure they do not breach the TPPs.
TPP 10 Quality of personal information	That the personal information about students or teachers that O365 or GAFE collects, uses, or discloses is not accurate, complete or up-to-date.
TPP 11 Security of personal information	That use of O365 or GAFE increases the risk of phishing, hacking or other security threats to the personal information of students or teachers. That Microsoft or Google staff gain inappropriate access to personal information about students or teachers that it holds through O365 or GAFE.
TPP 12 Access to personal information	That students and teachers do not get access to personal information about them that Microsoft or Google hold about them through O365 or GAFE.
TPP 13 Correction of personal information	That student or teachers are not able to correct personal information about them that Microsoft or Google hold about them through O365 or GAFE.

5. DISCLOSURE AND VISIBILITY OF PERSONAL INFORMATION OF STUDENTS AND TEACHERS EXTERNALLY

Use by schools of Cloud based applications such as O365 and GAFE involves Microsoft and Google respectively collecting significant amounts of information about students and teachers. This could include:

- content that a student has produced such as assignments, drawings, music, presentations etc and content that a teachers has produced, such as presentations, comments on assignments, assessment results, reports on students including disciplinary or counselling report
- communications via email, instant messaging, chat rooms, between students, between students and teachers, between teachers and between teachers and parents which could range between very personal non-school related topics through to very personal school related topics
- browsing history including searches, websites visited, click throughs, etc
- other metadata about interactions via O365 or GAFE including time, date, location, how long, who with, etc

Concerns, which have also been canvassed in the public arena have been about:

- the type of information about students (and teachers) GAFE and O365 collect use and disclose in the course of providing their tools and
- the purposes for which Google and Microsoft collect use and disclose this information.

This focus has arisen as a result of publicity over the last year (2013-14) which raises concerns that companies that provide these learning tools may be in a position to collect data about students' browsing habits (or other interactions) while they use these products, and subsequently build a profile which the companies can use outside these products while the person is still a student and also when the child becomes an adult.[1] In the US, for example, California's Assembly has approved first-in-the-nation privacy measures prohibiting the use of students' personal information for profit. The Student Online Personal Information Protection Act, when finalised "would end targeted advertising on K-12 websites, services and applications" and also "prohibits operators from using any information gained from the use of their K-12 site to target advertising on any other site, service or application."[2]

Google has been the main target for these concerns. However, this report considers this issue in relation to both GAFE and O365.

5.1 POTENTIAL HARMS AND RISKS

IIS has considered the most likely potential harms that could arise from the uses and disclosures of information about students or others in the educational context by applications such as GAFE or O365. This assessment takes into account the fact that neither O365 nor GAFE **displays** targeted

[1] See for example, Google admits data mining student emails in its free education apps, by Jeff Gould, President of Safegov.org, Friday 31 January 2014. http://safegov.org/2014/1/31/google-admits-data-mining-student-emails-in-its-free-education-apps

[2] http://sd06.senate.ca.gov/news/2014-08-25-first-nation-student-privacy-bill-approved-calif-assembly

advertising to students or teachers using O365 or GAFE core services while they are signed into the EDT environment. These potential harms and risks are:

- that information about students or teachers collected or stored within the ETD domain is used to target them when operating in the online environment outside the ETD domain
- that information about students (or teachers) is used to create a profile about each user – with the individual not having the chance to erase aspects of it that have changed, or that they might be ashamed of or could impede employment in the future. This can be a particular risk for students who may behave rashly or badly while young but grow out of those behaviours as they mature into adults
- that information about students might be disclosed to third parties for unrelated purposes
- that the holder of the information may decide to put the information they hold to new uses not contemplated at the time the information was collected. With use of big data approaches rapidly becoming the greatest source of value realisation for many organisations there may be strong incentives to use this information for new purposes with the data subjects having little chance to exercise control over such uses.

The next sections describe the privacy framework covering GAFE and O365 as they apply to the ETD rollout and discuss the extent to which each of the applications:

- creates unacceptable risk of harm to students (or teachers) from use or disclosure of student of teacher information
- may be breach of privacy law
- may give rise to perceptions of privacy harm and risk to ETD's deployment of the applications.

5.2 GAFE

5.2.1 Google Privacy Policy Terms of service

The terms and conditions that govern ETD's use of GAFE are set out in an online agreement at http://www.google.com/apps/intl/en/terms/education_terms.html. The terms of service were revised in 14 April 2014. This makes no reference to privacy apart from stating that "Google does not serve Ads in the Services or use Customer Data for Ads purposes." At the time of writing, these core services are Gmail, Google Calendar, Google Hangouts, Google Drive, Google Sites, Google Contacts, Google Apps Vault and Google Classroom. It provides for changes to GAFE Services and to URL terms (cl 1.2). It allows Google to make "commercially reasonable" changes to these services. If it makes material changes to services it must notify subscribers to Google of such changes.

Customers have the option not to take up changes to URL terms. However IIS is not aware of any URL terms applying to GAFE that relate to privacy.

Google also has generally applying terms of service which say that by using the service the user agrees that Google can use data in accordance with it privacy policy - https://www.google.com/intl/en/policies/terms/

Google's general Privacy Policy http://www.google.com.au/intl/en/policies/privacy/ sets out Google's general information handling practices. This appears to be mostly applicable to GAFE,

apart from the provisions that refer to the display of advertising and the user's interactions with advertisements. The Privacy Policy states that:

- its **purpose** of collecting information is to provide better services to **all** of its users, including figuring out the language the user speaks (it refers to targeting advertising as well but on the basis of statements elsewhere it is not applicable in this context)
- it **collects** information the user gives Google as well as the information that Google gets when the person uses the services for example, device information (Unique ID), log information such as search queries, IP address, browser type, and cookies; location information and cookies, how a user interacts with a site that uses Google advertising services
- it **uses** the information from all its services "to provide, maintain, protect and improve them, to develop new ones, and to protect Google" and its users. Improved user experience includes enabling services to appear in the user's preferred language and to make it easier to share information with people the user knows (and to display advertising the person is interested in but this is not applicable where advertising is switched off).
- it asks for **consent** before using information for a purpose other than those set out in the privacy policy
- it provides **choices** about use – review and control some information tied to the user's account, view and edit some preferences (e.g. advertising, if applicable), edit profile, control who information is shared with, take information about of services
- only **shares personal information** with organisations outside Google
    - with consent (opt-in where sensitive information involved)
    - with domain administrators (i.e. ETD administrators)
    - external contractors (under strict conditions)
    - legal reasons
- **shares aggregated**, non-personally identifiable information publicly (e.g. to partner publishers, advertisers or connected sites. For example it is used for Google Trends http://www.google.com/trends/ which displays hot search terms. (IIS understands that only high level data is taken from logs, such as search terms and mixed with the overall pool of Google search terms)
- it will **not reduce privacy rights** under the policy without the user's explicit consent.

5.2.2 GAFE – SECURITY AND PRIVACY DOCUMENT

This a specific statement about privacy and security in GAFE that Google has developed.

The document at www.google.com/edu/privacy.html states in relation to Gmail that:

- Ads in Gmail are turned off by default and that that Google has "no plans to change this in the future"
- Gmail scans and indexes email for multiple purposes, including spell check, virus and spam protection, Priority Inbox and auto-detection of calendar events and relevant search results (for example, which take into account spelling mistakes that the user makes, or knowledge that the student is looking for an animal jaguar rather than the car of the same name). Google does scanning to provide product features on all incoming emails and is 100% automated.

- Google does not scan GAFE core services for advertising purposes
- Google does not collect or use any information stored in GAFE users' Google Drive or Docs (or Sheets, Slides, Drawings, Forms) for any advertising purposes
- Google does not sell GAFE data to third parties and does not share personal information placed in their systems with third parties (except in a few exceptional circumstances, for example they have consent or they are required by law to do so and following a process of review and notice to the customer where possible).

It further states that the institution owns the data and that Google makes it easy for the institution to take its data away.

5.3 FINDINGS ON HARMS AND RISKS RELATING TO GAFE IN THE ETD ENVIRONMENT

5.3.1 TARGETING ADVERTISING OUTSIDE THE ETD ENVIRONMENT

IIS finds that:

- Google does not display advertisements to students or teachers when they interact with GAFE core services within the ETD environment. In addition, ETD administrators will not have the ability to turn on advertising display.
- Google has now permanently removed ads scanning in Gmail within GAFE – this means that it now does **not collect** information from Gmail that could be used for displaying tailored advertising from this source. However, it still collects search and browsing history which could potentially be used and analyses content when it is sent, received, and when it is stored.
- Google does not use information that it has collected through GAFE core services about students and teachers through the ETD environment to target advertising to students and teachers when they interact with Google products outside the ETD environment. Information in the ETD environment is "firewalled" within the ETD environment.
- If a student or teacher opens a separate Google account outside the ETD environment Google does not recognise that the student or teacher has a ETD Google account (unless the student or teacher adds the ETD email address as a second email address to their profile) and does not use any information it has gathered about the student or teacher within the ETD environment to tailor services, for example, search, to that separate Google account.
- Once a student or teacher is no longer an ETD student or teacher, Google does not use any of the information it has collected about the student or teacher in the ETD environment to tailor services, for example, search, to the ex-student or teacher who interacts with Google products.
- If a student or teacher is logged into their ETD account, but uses a Google service such as search outside the ETD environment using the same browser, Google service may not totally separate the two different sessions within the browser because of the cookies that GAFE has lodged in the browser.

IIS concludes that the risk of students or teachers being targeted with tailored services including advertising outside the ETD environment using information obtained through GAFE core services is very low taking into account Google's April 2014 announcement that it had removed scanning for

Ads purposes from Gmail. IIS considers that in this regard GAFE appears to fall within the use limitation requirements of TPP 6.

However, IIS considers that the barriers to wider uses are essentially policy decisions and undertakings made by Google rather than significant technology or engineering design barriers. For example, IIS considers that Google could potentially use unique machine identifiers to link data stored between the two Google accounts.

5.3.2 Building a profile of users for unrelated uses

IIS finds that GAFE builds up a profile about students that, with the exception of scanning for Ads purposes of Gmail which has now been removed, includes all the information that Google would collect if the student or teacher was interacting with Google products or services outside the ETD environment. It includes information gleaned from scanning and indexing content in Gmail (no longer for advertising purposes) and in Docs and Drive, logs of searches, location information, etc. However, the risks of Google using this information for purposes unrelated to the educational purposes of GAFE are mitigated by the following factors:

- Google's stated commitment to not use the information to target advertising and to limit its use to providing, maintaining, protecting and improving GAFE Service, to develop new ones, and to protect Google, which is deduced from a combination of the privacy policy, and the GAFE privacy and terms documents
- Google's commitment not to share personal information with advertisers or other third parties without consent
- Google's statement that Google anonymises log data by removing part of the IP address (after 9 months) and cookie information (after 18 months). See Privacy and Terms – Advertising http://www.google.com.au/intl/en-GB/policies/technologies/ads/
- when the student or teacher leaves ETD their account information, including user name is deleted after a short delay and log data is no longer associated with it
- users or their parents concerned about the privacy implications of this profile have a range of options that they can use to limit information collected through GAFE. These include:
    - Delete Web History – (including search history such as individual searches, all past searches) and to turn off web history to prevent future searches being stored). This means the information is no longer associated with the user's account, but Google may still store searches in separate logs system to prevent spam and abuse and to improve services. Options Google provides include to:
    - Delete browser history
    - Turn off location history and reporting
    - Delete the unique cookie ID assigned to the machine the first time it visited Google, although this will limited impact as it will be assigned a new one next time they visit Google from that particular machine.

5.3.3 Disclosing information for unrelated purposes

On the basis of the information IIS has, it finds that Google does not disclose personal information about students and teachers collected through the GAFE environment to advertisers or other third parties for purposes unrelated to the provision of GAFE services or other purposes beyond those allowed by TPP 6 relating to disclosure.

Google does share aggregated de-identified information drawn from browsing history and server logs with the public and some other organisations such as advertisers. On the basis of Google Trends as a typical example, it seems that very limited information, such as search terms and very limited geographic information, are drawn into Google's huge pool of similarly aggregated data, and as a result this constitutes a very low privacy risk to students and teachers. It is also consistent with Google's stated purpose of collecting information for the purpose of providing better services to **all** of its users.

5.3.4 FUNCTION CREEP – USE OR DISCLOSURE FOR NEW PURPOSES

Given the richness and potential value of the data GAFE collects about students and teachers, Google's business model, and the fact that GAFE is made available free of charge, IIS considers that use or disclosure of the data for new purposes is a risk that requires consideration. Because of the fairly undefined relationship between ETD and Google, ETD is reliant on the complex web policies and statements that Google has issued through its privacy policy, online agreement, and privacy and terms documents.

In particular, ETD does not appear to be in a position to prevent from Google using the information about students and teachers it holds for new purposes into the future, or from changing its approach to advertising.

Google states that it has no plans to change its approach to the display of advertising in the future. But this is simply a statement of intentions and does not rule it out altogether. Google also only undertakes to notify ETD should it make material changes to its service. There does not appear to be a chance for ETD to negotiate. Google says that it won't reduce the privacy undertakings in its privacy policy without consent, but this appears to apply to the user rather than the customer such as ETD.

Public opinion and the strong views of Google's clients may prevent unilateral changes to GAFE which reduce privacy undertakings. Indeed public pressure is leading to tighter rather than looser privacy protections. Nonetheless concerned parents, teachers or students may not find this a sound basis for reassurance.

5.3.5 PERCEPTIONS OF PRIVACY HARMS

A key risk for ETD is, regardless of the facts, public perception that GAFE poses a privacy risk particularly for students as a result of the significant information about students that it stores. IIS considers that this is not helped by the lack of clarity in, and complexity of, Google's privacy policy and other documents about what it does and does not do or may do in the future with the personal information it collects and stores in relation to GAFE. IIS acknowledges that GAFE is a complex product which makes simple explanation difficult. However the lack of clarity and complexity can leave the impression that Google is being less than completely transparent.

A key mechanism for protecting privacy is that of 'control' over personal information. A key mechanism for gaining and exercising that control is transparency. Through transparency, individuals can make decisions about whether to allow collection of their personal information. Even where an individual has no real choice about whether to provide personal information, transparency enables the individual to reassure themselves that information an organisation holds about them is properly managed. Transparency is also a requirement of TPP 5 which requires ETD to

tell parents, students and teachers that information about them is being collected through GAFE, the purposes for which it is being collected and the intended recipients of the information.

IIS considers that the information that ETD currently provide to parents, students and parents is not clear about the information Google collects from users of GAFE or the uses Google makes of it to meet the requirements of TPP 5. For example, it does not mention the server logs, browsing history and location information that will be collected and connected to the student's profile. In addition, IIS considers that the information is insufficient to place parents or students in a position to make an informed decision about whether they, or where applicable, their child, should use GAFE. In the circumstances, IIS considers that referring the parent or student to Google's privacy policy, which, in any case is not specifically tailored to GAFE, is too onerous and unlikely to be read or easily understood. The information does not mention that the information will be stored off shore or an access or complaints process.

An important aspect of the decision and ongoing use will be information about the options and choices that Google provides for those that have privacy concerns and also any other options they may be able to exercise via their browser. However, much of this is buried under multiple links and not necessarily where you would expect to find it.

5.3.6 RECOMMENDATIONS

5.3.6.1 RECOMMENDATION 1 – DEVELOP A CLEAR STATEMENT OF GOOGLE'S APPROACH TO PRIVACY IN GAFE

IIS recommends that ETD works with Google to develop a short but clear and accurate statement covering GAFE as rolled out by ETD that sets out:

- the kinds of information about users that Google collects through use of GAFE (including content, server logs, browsing history, location data and covering core and any additional services that are switched on)
- the purposes for which Google collects, uses and discloses such information
- the purposes for which Google will not use or disclose such information where that will add reassurance and clarity – for example, a statement that Google does not use GAFE information to tailor services when a user is interacting with Google products outside the ETD environment
- the fact that Google uses and discloses aggregate information drawn from logs for trend and other purposes and reassures that this is properly de-identified and cannot be associated with a user's account now or in the future
- GAFE's process and timing for deleting all the types of information about students and teachers it holds when a user become an ex-student or ex-teacher
- a statement (which should create as much certainty as possible) which indicates the extent of ETD and user control should Google decide to change its services or privacy policy in a way that has a detrimental impact on the privacy of ETD GAFE users
- an outline of the steps that ETD takes to assure itself that Google complies with its privacy undertakings outlined in the statement
- include the fact that information is stored offshore
- outline an access, correction and complaints process
- links to where the reader can get more information.

ETD should provide this statement to parents, students and teachers before ETD fully rolls out GAFE and emphasise the importance of reading the document before giving consent.

Recommendation 1 – Accepted by ETD

The ACT Education and Training Directorate implemented this recommendation by developing a Privacy Information Sheet for students and parents. The Directorate worked with Google and the NSW Department of Education and Communities to create this resource and ensure its accuracy. The document in its entirety can be found here: http://www.det.act.gov.au/__data/assets/pdf_file/0008/708839/DB-GAFE-Student-Privacy-Information-Fact-Sheet.pdf

Table 2 - Directorate comments against Recommendation 1

Recommended elements for the statement to address	Directorate Comments
• the kinds of information about users that Google collects through use of GAFE (including content, server logs, browsing history, location data and covering core and any additional services that are switched on)	Our privacy information sheet refers to the types of information being collected. Location History has also been disabled in the Directorate's Google Apps domain. *Use of Google Apps will mean that student personal information and data will be collected by Google for the purposes of providing the Google Apps services to students. This personal information will include the student's given name, surname, student ID number and all personal information that is contained in a Google Apps service; such as information or data contained in a student's calendar or email (including text, images, photographs, sound and multimedia).* *As part of providing its services, Google may also collect device information, log and location information as detailed in Google's Privacy Policy.* In addition, users (students and teachers) own their data in the Directorate's Google Apps for Education platform.
• the purposes for which Google collects, uses and discloses such information	Our privacy information sheet refers to the purposes for which Google collects, uses and discloses such information *Google stores and processes personal information solely for the purposes of providing the Google Apps service. Google scans Gmail to keep its customers secure and to improve their product experience. In Gmail for Google Apps, this includes virus and spam protection, spell check, relevant search results and features like Priority Inbox and auto-detection of calendar events. Scanning to provide product features is done on all incoming emails and is 100% automated.* Google also explicitly states the following in relation to the Google Apps for Education Service: *Google does not scan your data or email in Google Apps Services for advertising purposes.*
• the purposes for which Google will not use or disclose such information where that will add	Our privacy information sheet states that: *Google stores and processes personal information solely for the purposes of providing the Google Apps service.*

Recommended elements for the statement to address	Directorate Comments
reassurance and clarity – for example, a statement that Google does not use GAFE information to tailor services when a user is interacting with Google products outside the ETD environment	Due to public concerns relating specifically to advertising; We have also stated that: *Google Apps services do not collect or use student personal information and data for advertising purposes or to create advertising profiles.*
• the fact that Google uses and discloses aggregate information drawn from logs for trend and other purposes and reassures that this is properly de-identified and cannot be associated with a user's account now or in the future	Our privacy information sheet states that: *As part of providing its services, Google may also collect device information, log and location information as detailed in Google's Privacy Policy.* The Directorate also acknowledged the need for students to better understand and control their own personal data when interacting with online services. Therefore, additional resources have also been provided to parents and students on the Directorate's public DET Website page "Keeping Safe Online"
• GAFE's process and timing for deleting all the types of information about students and teachers it holds when a user become an ex-student or ex-teacher	Our privacy information sheet states that: *Unless required by law, Google will delete Customer-Deleted Data from its systems within 180 days of the ACT Education and Training Directorate deleting a student's account.* *Google will only disclose data at the direction of the ACT Education and Training Directorate or if compelled to do so by law.*
• a statement (which should create as much certainty as possible) which indicates the extent of ETD and user control should Google decide to change its services or privacy policy in a way that has a detrimental impact on the privacy of ETD GAFE users	The Directorate will continue to respond to the needs of students as it has always done. If Google were to change its privacy policy in a way that has a detrimental impact on the privacy of ETD GAFE users, students have the ability to delete any data in their account as well as download/export it as a self-service. ETD also has the ability to delete student accounts, which Google will then delete the Customer-Deleted Data from its systems within 180 days of the ACT Education and Training Directorate deleting a student's account, as stated in the privacy information sheet. There is also further evidence to support Google's commitment in Google's recent signing of the Student Privacy Pledge, where Google is held accountable to: *Not change privacy policies without notice and choice.*
• an outline of the steps that ETD takes to assure itself that Google complies with its privacy undertakings outlined in	The Directorate worked with other jurisdictions in consultation with Google to verify Google's privacy undertakings outlined in the Directorate's privacy information sheet. The Directorate will perform a bi annual review of the Google Terms and Conditions to ensure ongoing and consistent alignment with the Territory

Recommended elements for the statement to address	Directorate Comments
the statement	Privacy Principles.
• include the fact that information is stored offshore	Our privacy information sheet states that: *Google holds user data in its data centres that are located around the world.*
• outline an access, correction and complaints process	The Directorate has an existing process for all complaints and concerns, which is publicised on our public website under 'Concerns and Complaints': http://www.det.act.gov.au/contact_us
• links to where the reader can get more information.	Our privacy information sheet links readers to more information, including: ***Google Privacy Information:*** *Google's approach to privacy, security and transparency with Google Apps for Education is available at http://www.google.com/edu/privacy* ***Further Information:*** *http://www.google.com/apps/intl/en/terms/education_terms.html* *https://www.google.com/intx/en/enterprise/apps/terms/dpa_terms.html* *http://www.google.com/policies/privacy/* ***ETD Privacy Information*** *http://www.det.act.gov.au/functions/privacy*
• ETD should provide this statement to parents, students and teachers before ETD fully rolls out GAFE and emphasise the importance of reading the document before giving consent.	The Directorate has provided a release pack to all schools with a mandatory step-by-step process. GAFE will only be made available to a student whose parent/carer has been provided our information sheet and returned a signed parental consent form permitting their child to be provisioned into the Google Apps domain. We have designed Google in such a way that it is technically impossible to provision a student into our Google domain without the school applying parental permissions in the school's administration system first.

5.3.6.2 RECOMMENDATION 2 – INFORMATION TO PARENTS, STUDENTS AND TEACHERS ON PRIVACY OPTIONS

IIS recommends that ETD provide information that is easy to access, read and understand about the privacy options available to users both within GAFE or using other mechanisms such as those available through browser settings and use of browser sessions.

Recommendation 2 – Accepted by ETD

Directorate Comments:

The Directorate has provided simple and helpful information on available privacy options on their public DET website: *'Keeping Safe Online'*

http://www.det.act.gov.au/teaching_and_learning/learn-anywhere-ict-for-students/keeping-safe-online

Contained within this site is information on Google Apps for Education and Google Chrome: Privacy Options Including links to:

Manage your cookies and site data in Google Chrome:
https://support.google.com/chrome/answer/95647?hl=en

Delete your cache and other browser data in Google Chrome
https://support.google.com/chrome/answer/95582?hl=en

5.4 O365

5.4.1 Microsoft Office 365 privacy framework

The following is the framework within which Microsoft manages the personal information it collects, uses, stores and discloses through Microsoft Office 365.

Microsoft has entered into a licence agreement with ETD to gain the licence to make Microsoft Office 365 available to students and teachers.

Microsoft also provides for optional privacy and security contractual supplements that ETD could sign up to. For example, one of these applies to customers outside Europe and specifically relates to data processing Office 365 Security Amendment (for customers outside of Europe) [English]. It states that Microsoft:

- complies with all laws generally applicable to its services
- will not require any rights in Customer data
- will only use or disclose Customer data for the following purposes :
    - to provide ETD with the Microsoft Office 365 services, which may include trouble shooting aimed at preventing, detecting and repairing problems affecting the operation of the services and the improvement features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam)
    - where required by law, for law enforcement purposes – following a specific process outlined which begins, where possible with directing the agent to ETD.
- outlines its approach to deletion of customer data on termination of ETD's use of Microsoft Office 365
- personnel will not process Customer Data without customer authorisation and are obliged to maintain the confidentiality of any Customer Data.

Microsoft says that these supplements simply set out the way that as a matter of policy and practice, Microsoft handles information relating to Office 365.

5.4.2 SUPPORTING DOCUMENTATION

Microsoft supports the contractual provisions with more simply expressed documents that are an accurate statement of the provisions in the contract. These are placed online in a place called the Trust Centre. Key documents for Office 365 include:

- Office 365 Privacy Statement http://www.microsoft.com/online/legal/v2/?docid=22&langid=en-us
- How we use your data http://www.microsoft.com/online/legal/v2/?docid=23
- Your Privacy Matters: We respect your privacy http://office.microsoft.com/en-us/business/office-365-cloud-privacy-FX103046091.aspx

All these documents reinforce the same statements of the Microsoft approach which is:

- it uses the user data to maintain and provide Office 365
- it is Microsoft's policy not to use user data for other purposes
- Microsoft 365 (as a business service) is designed and operated physically and logically separately from Microsoft's consumer services (i.e. Hotmail, etc)
- Microsoft does not scan emails or documents for advertising purposes.

It provides a table that sets out its use of Customer Data (which does not include operational information i.e. logs about the service)

Table 3 - Microsoft Office 365 use of Customer Data

Use of Office 365 Online Customer data	**Customer Data (excluding content)**	**Content**
	text, sound, software, image files that user provides or are provided on user's behalf	(Subset of customer data) considered confidential, sent encrypted, includes email body and attachments, SharePoint Online site content (not URL), file body, instant messaging body, voice conversation, CRM files containing info about user end customer interactions
Service operation and trouble shooting	Yes	Yes
Security, spam and malware prevention	Yes	Yes
Services Communications	Yes	No
Improving the purchased services	No	No
Advertising	No	No
Voluntary disclosure to law enforcement	No	No
Direct marketing	No	No

The *How we Use your Data* document also indicates in relation to personally identifiable information about end user's interactions with services: "usage data" or ancillary data. It says that it may use

such data for day-to-day operations and maintenance of the Office 365 Services and for services communications to administrators, for example, about usage limits being reached. Microsoft also keeps this data separate from consumer data. This data includes IP address, audit reports. This is stored in raw format in a data centre with very limited access for security purposes. Microsoft has strict processes for such access. For operational analytics the data is stripped of personally identifiable information and encrypted.

The document also states that:

- Access to customer data is strictly controlled and logged, and sample audits are performed by both Microsoft and third parties to attest that access is only for appropriate business purposes
- If someone such as Microsoft personnel, partners, or administrators access a user's content on the service, it can provide the user with a report on that access upon request.

Microsoft spells out these commitments in its White Paper *Privacy in the Public Cloud* http://www.microsoft.com/en-us/download/confirmation.aspx?id=28540

It supports these commitments through a security, audits and certification program described at http://www.microsoft.com/online/legal/v2/?docid=27 including ISO 27001. This states that Microsoft conducts third-party audits and certifications to establish that its services are designed and operated with stringent safeguards. It aims to give accurate assurances about its security and privacy practices. It also states that Microsoft implements and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction. Every year, it undergoes third-party audits by internationally recognized auditors as an independent validation that it complies with its policies and procedures for security, privacy, continuity and compliance.

5.5 Findings on harms and risks relation to Microsoft Office 365

5.5.1 Targeting advertising outside the ETD environment

IIS finds that Microsoft has made clear commitments that it does not collect or use information through Microsoft 365 for advertising purposes. This includes content and ancillary "usage" data. This is supported and assured by the controls it has in place and the third party audits it conducts. In addition, there are logical and physical barriers which would make it very difficult for Microsoft to use the data it collects through Microsoft Office 365 outside the ETD environment for its consumer services.

IIS finds that there is no risk of students and teachers being targeted for advertising when they interact with Microsoft Office 365 within the ETD environment and no risk of students or teachers being targeted with tailored advertising outside the ETD environment using information collected through Microsoft Office 365. It falls within the use limitation requirements of TPP 6.

5.5.2 Building a profile of users for unrelated purposes

IIS finds that Microsoft builds only a very limited profile about Microsoft students and teachers. It does not provide the kind of services that would involve collection of such information as search terms that could enable it to provide a rich profile that might be valuable for unrelated commercial

uses. It de-identifies its usage logs for use for general operational purposes and imposes audited restrictions on access to the raw logs. Its clear commitment in its contract with ETD to only use and disclose information for the purpose of providing Office 365 services ETD and its control and audit regime also provide reassurance.

5.5.3 Disclosing information for unrelated purposes

IIS finds that Microsoft does not disclose personal information about students and teachers collected through Office 365 to advertisers or other third parties for purposes unrelated to the provision of Office 365 services beyond those allowed by TPP 6 relating to disclosure.

Microsoft has made clear commitments in its documents to limiting its disclosures to those for the purpose of providing the services and law enforcement purposes if required by law. This is supported by controls and third party audits.

5.5.4 Function creep – use or disclosure for new purposes

IIS finds that the chance of Microsoft unilaterally changing its approach to use and disclosure of personal information within Microsoft 365 is very low.

5.5.5 Perception of privacy harms

IIS considers that risks of perceptions among parents, students and teachers of privacy harms associated with use of Microsoft 365 is also very low. This can partly be attributed to the fact that Microsoft has set out to build Privacy by Design into all its cloud services both at a policy and at an engineering level. This has involved making a clear separation between its business services and its consumer services such as Hotmail and Bing. It has also involved developing a clear message about what it will and what it will not do which is based on a purpose which is limited to use and disclosure to provide the services sought. Its business model for these services is not based around deriving commercial benefit from the data collected.

Although Microsoft does have good material online that presents information about the way it manages privacy within Office 365. The *Microsoft Office Trial Privacy Information and Consent Form* that ETD has used for its pilots is a good model.

5.5.6 Recommendations

5.5.6.1 Recommendation 3 – Privacy notice

IIS recommends that ETD amends its O365 Privacy Information and Consent form that was used in the trial to ensure that it complies with the notice requirements outlined in TPP 5. For example, it should include information about access, correction and complaints processes.

Recommendation 3 – Accepted by ETD

Directorate Comments:

The Directorate has developed a new Privacy Information Sheet for Microsoft Office 365 in compliance with the Territory Privacy Principles. The document is available here: http://www.det.act.gov.au/__data/assets/pdf_file/0007/708838/DB-0365-Studenty-Privacy-Information-Fact-Sheet.pdf

5.5.6.2 RECOMMENDATION 4 – CONTRACTUAL SUPPLEMENT

IIS recommends that ETD enter into a contractual supplement similar to the one that Microsoft has developed for customers outside Europe (Office 365 Security Amendment (for customers outside of Europe) [English]) which includes provisions that limit its use and disclosure of the personal information it holds in relation to O365.

Recommendation 4 – Accepted by ETD

Directorate Comments:

The Directorate has enacted the Office 365 Security Amendment (for customers outside of Europe). This amendment applies additional measures to limit use and disclosure of personal information within Microsoft Office 365.

5.5.6.3 RECOMMENDATION 5 – INFORMATION TO PARENTS, STUDENTS AND TEACHERS PRIVACY OPTIONS

IIS recommends that ETD provide information that is easy to access, read and understand about the privacy options available to users both within Microsoft 365 or using other mechanisms such as those available through browser settings.

Recommendation 5 – Accepted by ETD

Directorate Comments:

The Directorate has provided simple and helpful information on available privacy options on their public DET website: *'Keeping Safe Online'* in the section 'Microsoft Office 365 and Internet Explorer: Privacy Options' including links to:

Delete and manage cookies in Internet Explorer: http://windows.microsoft.com/en-au/internet-explorer/delete-manage-cookies#ie=ie-11

Change privacy settings in Internet Explorer: http://windows.microsoft.com/en-au/windows/change-internet-explorer-privacy-settings#1TC=windows-7

View and delete your browsing history in Internet Explorer: http://windows.microsoft.com/en-au/internet-explorer/manage-delete-browsing-history-internet-explorer#ie=ie-11

6. DISCLOSURE AND VISIBILITY OF PERSONAL INFORMATION OF STUDENTS AND TEACHERS INTERNALLY

ETD is still in the process of developing the detail of how it will implement O365 and GAFE for the full roll out to schools. Since IIS does not have the detail, this section is a high level assessment of the possible risks related to internal use and disclosure of personal information about students and teachers and provides high level advice about how to go about minimising these risks.

Both O365 and GAFE are designed to enable collaboration and communication between students, and students and teachers, and also to some extent with parents. Depending on how ETD configures the applications and services students, teachers, and potentially parents could be aware of a whole range of information about each other that was not available before including:

- the email addresses of everyone in schools in the ETD system
- each other's text, voice or video chat conversations
- each other's documents, presentations, sites or material that teachers post

- comments that people including a teacher has made on a shared document or in another forum where views are shared
- whether a person is online and available to communicate (at any time of day or night)
- each other's appointments or meetings

Access to much of this could also be facilitated through the enhanced search mechanisms that are provided.

It is certainly the case that not every student and every teacher needs access to all of this information in order to achieve the necessary level of collaboration and learning outcomes. At the same time, the risks and possible harms of sharing more than is necessary of this information include:

- widening the channels and scope for harassment or bullying or abuse or unwanted or annoying communications
- mistaken or deliberate intrusion into private or sensitive communications between students and teachers, or between teachers or between students
- enabling insights about a student's or a teacher's life (for example, their location or at what times of the day they are online revealing when and for how long they work) that others may not need, or don't need to know about
- providing insights into private appointments or meetings that others don't need to know about.

The ETD document *Communities online: Acceptable use of ICT – Parents and Students Guidelines* October 2013, has clear policies and procedures on inappropriate use in the online environment. However, IIS considers that where possible ETD and / or schools should seek to implement technical steps that will help to minimise the risks outlined. O365 and GAFE have built in sharing permission controls and other administrative tools to restrict who has access in relation to a particular application or service.

IIS advises that ETD consider taking the following steps to manage the risk of inappropriate internal use or disclosure of personal information in relation to O365 and GAFE:

- consider each of the applications or services that O365 and GAFE provide
- assess against the collaborative and educational goals of ETD the extent to which users of the particular applications or services need access to information about other users
- identify the tools that each application or service makes available to limit access to those with the identified need
- identify other tools that ETD could use to limit access
- consider which of the tools should be applied and to which groups, and how restrictive they should be taking into account such matters as:
    - the likelihood and severity of harm to students and/or teachers from not restricting access
    - the likelihood and severity of harm to students and/or teachers from restricting access, including the duty of care to students

- the need for flexibility to respond to changing circumstances and the ease with which settings can be changed to respond to changing circumstances

In the case of email for example, it is unlikely that every student will need every other student's or every teacher's email address. ETD could therefore create security/distribution groups to limit access to the emails of other users.

In the case of indicators that a person is online or not, ETD could investigate whether it is possible to mask this, for example, outside school hours.

Disclosure and Visibility of Personal Information of Students and Teachers - Accepted by ETD

Table 4 - Directorate comments against recommendations regarding disclosure and visibility of personal information of students and teachers internally

Recommended considerations for the disclosure to address	Directorate Comments
• consider each of the applications or services that O365 and GAFE provide and identify the tools that each application or service makes available to limit access to those with the identified need	The capabilities of both Google Apps for Education and Microsoft Office 365 were assessed in a trial of eight schools. As part of this trial, schools identified which of the capabilities were of the highest value to students and teachers for teaching and learning. The trial validated a configuration of the platform to enable the Directorate with granular controls over which services are made available only to those with identified need. For e.g. Google+ is Google's social networking platform and is disabled for all Primary School students. However, there is a genuine need for teachers in the system to have social enterprise collaboration capabilities, therefore Google+ Communities was made available only to teachers.
• assess against the collaborative and educational goals of ETD the extent to which users of the particular applications or services need access to information about other users	As a result of the trial, it was determined that students and teachers needed varying permissions of access to contact information of others in the domain. - Teachers need access to contact information of students at their school only. It was identified that teachers should also have the ability to collaborate with other teachers in the Directorate for the purpose of school network, collegiate and jurisdictional communities of practice. - Students need access to contact information of their individual teachers and students in their class only. Given these requirements, the Google Apps platform was set up in the following way: - The user contact directory in Google enables all

Recommended considerations for the disclosure to address	Directorate Comments
	users to see everybody, such as every student in every school; therefore this directory was disabled. Instead, groups and permissions were established so only teachers could communicate with students at their school in logical groups such as all students, year groups, classes and units. Students were only given access to a group which enabled them to contact their class, which would always include their teacher. Microsoft Office 365 has a similar contact directory for the entire Directorate's tenant/domain. However, it was not technically possible to separate this directory in 365 between schools. Therefore the "email" and "people/contacts" component was disabled in Office 365, as was the SharePoint Online capability which would enable online web collaboration. Feedback from the trial indicated that Google Apps should be the platform where this functionality was enabled.
• identify other tools that ETD could use to limit access	The Directorate's identity system uses SAML Single Sign-On technology to restrict Google and Microsoft from obtaining student and teacher login passwords. All students and teachers login to the platforms internally and are then automatically authenticated into the platform. More information on SAML SSO in Google and Microsoft platforms: https://developers.google.com/google-apps/sso/saml_reference_implementation http://blogs.office.com/2014/03/06/announcing-support-for-saml-2-0-federation-with-office-365/ Other supported tools were used with our implementation of Google Apps to prevent teachers and students any ability to move their own accounts to other schools or groups within other schools in an attempt to gain access or visibility that shouldn't be accessible to them. We have implemented the system so it is not possible for a teacher or student to do this. The only way students and teachers are moved is via an automated process which synchronises the Google environment with the school's administration system database. This means that a student can only be moved to another school if the other school enrols this student in the administration system.

Recommended considerations for the disclosure to address	Directorate Comments
• consider which of the tools should be applied and to which groups, and how restrictive they should be taking into account such matters as: o the likelihood and severity of harm to students and/or teachers from not restricting access o the likelihood and severity of harm to students and/or teachers from restricting access, including the duty of care to students o the need for flexibility to respond to changing circumstances and the ease with which settings can be changed to respond to changing circumstances • In the case of email for example, it is unlikely that every student will need every other student's or every teacher's email address. ETD could therefore create security/distribution groups to limit access to the emails of other users.	The **Google Apps** Organisational Structure was established to enable granular controls over the availability of services to varying groups of students and teachers. Services/Tools can be enabled or disabled to the following groups: - entire school - all students and all teachers in an ACT Public School - all staff at a school - all students at a school - all students in a year cohort within a school. It is not technically possible to enable/disable a service for individual students or teachers. This structure has allowed for the Directorate to apply default controls such as: - Google+ and Google Hangouts are disabled for all students in all schools, but is enabled for teachers. - the ability to create a YouTube account and video channel is disabled for Primary School students. - the Chrome Web Store, which enables third party apps to be installed to the user's Google Chrome browser has been disabled for students and enabled for teachers. It is possible for a school to request a change for their specific school, such as disabling email for Years K-4, or enabling Google+ for Year 11 and 12. This must be authorised by a Principal who will endorse a genuine educationally viable purpose for the service change. Schools are advised to work with their parent community as participants to such decisions in relation to any service changes which could present a risk to student's privacy. The email user directory has been disabled. Users are unable to query the directory for contacts in other schools. The established configuration allows for flexibility and ongoing changes/updates to the service offering. The Directorate will continue to monitor the use of services in the domain and consider any changes based on the needs of schools in consultation with their parent community, and consideration to privacy and risk mitigation strategies. In the **Microsoft** platform, the Directorate has enabled Microsoft Office Online and OneDrive for Business, which provides the full office suite live in the browser including online storage.

Recommended considerations for the disclosure to address	Directorate Comments
	It was not possible to apply granular controls (out of the box) to customise the visibility of schools in the Microsoft SharePoint Online service, nor the Exchange Online service. Therefore, SharePoint Online, Exchange (email) Online, Lync Online (video, IM chat and online presence) and People (contact directory) are disabled.
• In the case of indicators that a person is online or not, ETD could investigate whether it is possible to mask this, for example, outside school hours.	The capability of 'Online Presence' which provides the ability to see if a user is online and to communicate with them is provided in both Office 365 with 'Lync Online' and Google Apps for Education with 'Google Hangouts'. Both services have been disabled for students. Google Hangouts is available for teachers and if a web/video conference is required, teachers are able to facilitate this for their class under their account to ensure the appropriate duty of care for these activities.

7. OTHER KEY ISSUES OR RISKS

This section identifies other key risks or issues arising from the TPPs that ETD should consider in implementing O365 and GAFE in schools.

7.1 TPP 1.3 – 1.4 PRIVACY POLICY

IIS has read ETD's privacy policy and advises that once ETD has implemented O365 and GAFE it should revise its policy to include information about the way it manages any risks arising from use of these applications/services. It should include specifically the fact that information about students and teachers collected via O365 and GAFE is stored offshore. IIS suggests that ETD consider having a privacy policy that is specific to schools, rather than a generic one for the entire Directorate. This would enable ETD to provide more specific information in the one place about how it handles personal information of students, and in particular, in relation to O365 and GAFE.

Privacy Policy Advice – Advice partially accepted by ETD

Directorate Comments:

The Directorate has implemented the recommendation to provide clear and concise privacy information in relation to O365 and GAFE by developing the privacy information sheets for both Google and Microsoft services. These sheets include statements to inform parents that information will be collected and stored offshore in order to provide the service. Schools are only able to enable the services for students who return a signed privacy consent note from a parent/carer, which is to be distributed with the privacy information sheet.

The Privacy Policy for all of ETD as an organisation will remain as a single policy for both schools and the Directorate itself. IIS recommended that ETD create a specific policy just for schools to be more specific of how student information is handled, particularly in relation to O365, GAFE and other third party web services. Instead of this approach, the Directorate now requires all schools to provide parents with specific information relating to any third party web service that the school seeks to use for teaching and learning and to seek parental consent before enabling any third party service that requires the use/disclosure of student personally identifiable information. Such information should include what student personal information is required in order to provide the third party service, what that information will be used for and if it can be disclosed to subsequent third parties.

7.2 CONSENT

IIS has noted that taking into account the legal advice that ETD received, ETD is proposing to gain written consent from parents to their child being signed up to O365 and GAFE. This is certainly best practice if the main goal is to enable ETD to establish that it has gained consent should there be any questions raised about this. However, from the point of view of the user, such as a student or teacher or parent, the key privacy protection is to be given real and informed choice about whether or not to use, or allow their child to use these applications/services.

Parents or students will not have real choice if a decision not to participate results in effective exclusion of the student from key educational activities. Providing information that ETD has thoroughly assessed the risks and has measures in place to handle them is likely to reassure most parents and so a decision not to consent is likely to be rare. However, to ensure real choice, ETD must also be in a position to ensure that students that do not participate in O365 or GAFE will not be substantially disadvantaged. ETD should consider providing a policy direction about this.

Choice should be partnered with easy to read and understand information of the kind identified above about O365 and GAFE. This information should also be provided in a just in time mode near to where the person first enters the O365 or GAFE application/service.

Consent Advice – Advice accepted by ETD

Directorate Comments:

The Directorate has established a system to ensure parents are provided clear information on privacy in relation to the use, disclosure and storage of personal information in GAFE and O365. This provisioning system is such that GAFE and O365 cannot be enabled for a student until parental permission has been applied in the student administration system. The system and processes implemented are as follows:

- A school principal must submit a form to the Directorate, acknowledging their responsibility to seek informed parental consent from parents prior to enabling the service.
- After the form is submitted and acknowledgement is verified, the Directorate adds two permission fields in the student administration system, which will be stored in the same section as other parent permissions for each individual student. The permission fields are:
    - Google Apps for Education - Parent Permission
    - Microsoft Office 365 - Parent Permission
- By default, the permissions are set to “No”. The school undergoes community consultation in seeking informed parental consent from parents/carers. This includes at minimum:

- A letter explaining the ICT vision at the school, the school's intent to adopt GAFE/O365, request for permission and statement that if permission is not provided then the school will ensure their child is not excluded or disadvantaged and alternatives will be discussed in order to achieve the same learning outcomes for their child.
- A copy of the privacy information sheet for the relevant platform to provide parents with informed choice.

- The school will receive the signed consent form and update the parent permissions accordingly. When a parent/carer has given permission and the school updates the permission to "Yes", the system will automatically provision the student into the platform. This initial provisioning process is expected to take approximately 3 days until the service is available in the student's Digital Backpack (online services portal).
- It is possible for a parent to rescind their permission at any time by contacting the school. If the permission is update from "Yes" to "No", the student will be de-provisioned access and the account can then be deleted from Google upon request of the parent.

7.3 Privacy protection generally and cloud service providers

In implementing O365 and GAFE and consideration for ETD will be whether using these cloud services, which also involve storage of personal information offshore, will increase the risk of privacy or security breaches such as unauthorised access from either internal Microsoft or Google personnel, or from external service providers or from hackers with malicious intent. This is of particular importance in relation to such sensitive information as counselling reports, behaviour and discipline reports, course assessments or information about children in need of care. ETD will need to consider such matters as whether:

- Microsoft and Google have adequate policies procedures and systems for protecting personal information of students and teachers from unauthorised access by Microsoft and Google staff
- Microsoft and Google have adequate policies, procedures and systems to protect its systems from malicious external attacks such as hacking, socially engineered attacks
- the nature of the undertakings that Microsoft and Google are prepared to enter into in relation to these matters.

To assess whether there is an increase in risk, ETD would need to compare Microsoft and Google's policies, procedures and systems with those that would be in place if the information was stored in facilities more directly under ETD's control.

IIS is not in a position to make a detailed finding on this issue. However, IIS observes that while both Microsoft and Google make statements which reflect a commitment to protecting the privacy and security of the information they hold through O365 and GAFE, Microsoft is much more up front transparent about the mechanisms it has in place to achieve that end and is prepared to enter into specific contractual undertakings about its approach. In contrast, for example, Google relies heavily on its privacy policy to outline its approach to security in fairly general terms ("we work hard to protect . . . ",). Google's online agreement does not make any reference to, or undertakings about, security. However, Google does have a quite detailed and comprehensive document that outlines

its approach to security in a white paper that can be found with some searching[3]. IIS has not examined this in detail, but this appears to provide security measures similar to those of Microsoft. A key difference is that ETD will be better able to establish that it has taken contractual measures to ensure that Microsoft will not breach TPP 11 relating to security, and other relevant TPPs as required by s 21 of the Information Privacy Act, if it enters into a supplementary agreement, than it would in relation to Google. ETD would also be in a better position to establish that it has met the requirement of TPP 8.1. This TPP requires ETD, before disclosing personal information to overseas recipients, to take reasonable steps to ensure that the recipients do not breach the TPPs in relation to the information.

This could be a relevant consideration when deciding, or developing guidance about, where student or teacher information should be stored, particularly where sensitive information is involved.

Privacy Protection Generally and Cloud Service Providers Advice – Advice accepted by ETD

Directorate Comments:

Noted considerations stated by IIS:

- Microsoft and Google have adequate policies procedures and systems for protecting personal information of students and teachers from unauthorised access by Microsoft and Google staff
- Microsoft and Google have adequate policies, procedures and systems to protect its systems from malicious external attacks such as hacking, socially engineered attacks
- the nature of the undertakings that Microsoft and Google are prepared to enter into in relation to these matters.

Further research has been conducted in relation to the policies, procedures and security protocols undertaken by Microsoft and Google to protect our information. The Directorate concludes that the security models in place with both vendors are as robust as our own.

Further information on the security of Google and Microsoft cloud services are below. Some of this information has also been provided in the Privacy Information Sheet for parents.

Google's physical data centre access is restricted to authorised personnel and multiple layers of physical security are implemented, including manned security and biometric scanning. Google personnel are only able to access user data in extremely limited circumstances and subject to rigorous approval and oversight.

Google customer data is broken up into multiple layers and split from data layers and application layers. This means that any hard drive in any Google data centre is humanly unreadable as it is not presented in plain text. Additionally, individual hard drives only contain byte fragments of data that cannot be associated to any user or any specific Google service. Hard drives that are defective and do not pass regularly scheduled reliability diagnostics are physically destroyed on site. Data is unable to be retrieved once destroyed.

Google Apps and Google Cloud Platform are certified for SSAE 16/ISAE 3402 Type II, received the SOC2 audit and the ISO 27001 certification. This means that an independent auditor has examined the controls protecting the data in Google Apps (including logical security, privacy and data centre security) and assured that these controls are in place and operating effectively

Physical data centre access for Microsoft is restricted to authorised personnel and multiple layers of physical security are implemented. This security practice is consistent with the practices used by ACT Government.

3 http://www.optusbusiness.com.au/office/Security_Whitepaper_Google_Apps_Messaging_Collaboration_products.pdf

Personnel are only able to access user data in extremely limited circumstances and subject to rigorous approval and oversight. Microsoft use subcontractors to perform a variety of support services for O365. Examples of these include, physical hardware maintenance, technical support and facilities services (e.g. security guards at data centre locations).

Current Directorate policy is that sensitive personal information and sensitive corporate information should not be stored in Google, and that local ACT Government network drives should be used for this purpose. Such information includes counselling records, financial records, HR and student records which would otherwise be stored in the secure file at the school.