Aberdeen City Deployment of Google Apps for Education

Privacy Impact Assessment Screening Questions

BON ACCORD

ABERDEEN
CITY COUNCIL

0.1 About this Document

This document records the work undertaken by Aberdeen City Council - Learning Technologies Team in relation to a Privacy Impact Assessment for Google Apps for Education.

0.2 Revision History

Version	Date	Summary of Changes
1.0	30 November 2014	

0.3 Distribution

This document will be distributed to:

Name	Title	Version

Introduction

The Aberdeen City Council is committed to ensuring that our public services are high quality, continually improving, efficient and responsive to local people's needs. To do so we need to reshape our services to deliver better outcomes for learners, parents, teachers and other professionals but at a reduced overall cost. There is a need for more collaboration, more cooperation, and more sharing of resources and services.

In doing so, we need to ensure that people's personal data is handled with respect and alignment with relevant legislations and other appropriate guidance principles. Respect for privacy should always be central to the way in which public services manage people's identity information.

Looking after the citizen's data is also part of good administration, efficient service delivery, and respect for clients.

The purpose of this report is to report on and assess against any potential Privacy Impacts as a result of deploying 'Google Apps for Education[1]'.

1.0 Executive Summary

A Privacy Impact Assessment[2] is a cyclical process. It initially requires the organisation to answer a number of screening questions to determine the need for a PIA or not.

Google Apps for Education is a cloud based service, which may store limited personal information related to every school age user and staff member across Aberdeen City's Education Service. Considering the limited sensitivity of this information and the limited scale of the technical solution, it was determined that a privacy impact assessment would not be required however a number of user communications and activities would be used during the adoption of the solution to ensure users were aware of potential risks.

It is clear from the information gathered that the technology provider complies with high standards of data security, and that sound procedures are in place for the storage, retention and deletion of data held. That said there remains a low level of risk due to the nature and volume of the data held. A number of communications activities will be undertaken, to ensure that users are aware of the types of data held, and how they should make best, safe use of the system. A number of communications products, including 360 Degree Safe[3], will be delivered to ensure that different audiences (technical, young person, adult) have the information they need.

[1] http://www.google.com/enterprise/apps/education/

[2] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[3] http://www.swgfl.org.uk/360

2.0 Privacy Impact Assessment

A Privacy Impact Assessment[4] (**PIA)** is a risk management technique for projects or policies that involve personal information or intrusive technologies, conducted to identify and address privacy issues.

A **PIA** is a process which is conducted at an early stage of a new project / policy or when a considerable change to a project / policy is planned. As policy progresses into the development and implementation stages the PIA is revisited, reviewed and refined to inform and ensure an on-going relevance and compatibility with technological and legislative developments. A PIA is a requirement for all projects which have a potential impact on personal privacy.

A **'Potential impact'** can be a positive or negative effect on individual privacy, and these impacts should be considered in the widest possible context - it may be that an initiative which on its own is relatively neutral may combine with other factors to impact (positively or negatively) on the privacy of the individuals affected.

Personal privacy is meant in a wide sense: the holding of information about the citizen, the perception of the citizen about the degree of surveillance or oversight they are under, and includes the effects on the citizen's personal dignity as they come into contact with an organisation or public body.

2.1 PIA – What's Involved?

The Information Commissioner's office (ICO) PIA Code of Practice identifies 7 discrete steps in the PIA process, noting that the PIA is a continuing and cyclical process:

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process

.

This report, in essence, documents the initial identification of the need for a PIA or not for the implementation of Google Apps for Education in Aberdeen City Council.

In addition to following ICO guidance the report will also, where applicable, make reference to the following:

[4] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

- 8th principle of the Data Protection Act 1998 (international data transfers)[5]
- The Scottish Government's Identity Management and Privacy Principles (2011)[6]

3.0 Preliminary

The deployment of Google Apps for Education is a project run by the Learning Technologies Team within Aberdeen City Council.

Clearly identified governance arrangements; defined roles and responsibilities, effective management controls and quality assurance processes ensure effective delivery of a piece of work.

Tasks associated with the delivery of a PIA have been identified and assigned to the relevant staff within the Learning Technologies Team. Progress on these tasks is managed and reported on in relation to Aberdeen City Council practice and procedures.

3.1 Initial Assessment

The ICO guidance outlines the requirement for an Initial Assessment[7] of privacy issues to decide whether a PIA is required. The initial assessment should be informed by the project outline; stakeholder analysis; external information gathering; the PIA Screening Process to determine whether a small scale or a full scale PIA is required.

3.1.1 Introduction

The initial assessment for a PIA for Google Apps for Education was undertaken in November 2014. It looked at the outline of the project; analysed the stakeholders involved in the project; examined what external information was required to set the project in the appropriate context; and finally undertook the PIA Screening Process using the ICO Screening Questions to ascertain whether a PIA was required. The initial assessment is described below.

3.1.2 Project Outline

Aberdeen City Council intend to deploy Google Apps for Education (GAFE). The services with in GAFE are to be managed and deployed by the Learning Technologies Team to education users. Over time and with appropriate training in place, school technical staff will be provided with the tools to manage their own Organisation Unit within GAFE.

We intend to store the minimum amount of user information, for the purpose of authentication, in Google Apps for Education This information will is held securely in GAFE and will be an extract of the data currently held within the Glow Service. Usernames will be that same in GAFE and in Glow.

[5]]http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/international_transfers_legal_guidance_v3.0_171208.pdf

[6] http://www.scotland.gov.uk/Resource/Doc/82980/0116729.pdf

[7] http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/2-Chap3.html

3.1.3 Stakeholder Analysis

The purpose of this analysis is to identify all groups or organisations who may have a interest or role to play in delivering this project or be affected by it.

Learners with in Aberdeen City Council

Young people from early years to S6 may be provided with access to GAFE for learning activities and communication.

Teaching Staff in Aberdeen City Council

All teaching staff will be provided with access to GAFE for learning activities and communication. Staff will be encouraged to share resources with other teachers and learners via GAFE.

Learning Technologies Team with in Aberdeen City Council

The Learning Technologies will manage the deployment of GAFE and provide training to users relating to learning and teaching with Google Apps for Education.

Corporate ICT Team

Technical support to ensure required ports and endpoints for authentication and services are unblocked. Also, the Support Analyst Team may be involved in the administration of some Organisational Units.

External Groups and Individuals (including Learners Post School, Aberdeen College, University partners)

Post school learners may wish to access their own content. Other partners may make use of the service for projects linking with Aberdeen City Schools. There will be limited and time sensitive access to GAFE for these users.

National Agencies (including Education Scotland, SQA, Scottish Government)

The national authentication service for Glow will provide user data services for Google Apps for Education.

Service providers (including RM Education Ltd)

External service providers may have a role in providing elements of the authentication data within Glow. For example: RM Education Ltd are the service provider the national Glow authentication who already make the data required available via download from the RM Unify Management Console.

3.1.4 Screening Questions

The ICO recommends undertaking a PIA screening process using the Privacy impact assessment screening questions'[8] to establish if a PIA is required. The purpose of the screening process is to ensure that the investment the organisation makes is proportionate to the risks involved. There are eight questions involved in the screening process.

3.1.5 Reponses to Privacy Impact Assessment Screening Questions

Q. Will the project involve the collection of new information about individuals?

A. No, the data held about individuals will be the same as that held in the National Glow Service.

Q. Will the project compel individuals to provide information about themselves?

A. Users may be compelled to share location data to access features of services such as Google Maps and administrators may access user location data as part of device monitoring however users using laptop/desktop systems will have the ability to choose to share their location or not. No other information will be required and users will not be required to provide further personal data to use the service.

Q. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Yes, information will be available to Google in line with the terms and conditions of use of Google Apps for Education. Google undertake not to process the data within GAFE for marketing and adverts are not shown to GAFE users.

Q. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

A. The information required is already used to provide the national Glow authentication service. The information will be used to provide an additional account enabling access to Google Apps for Education.

Q. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

The proposal makes two changes that change to the handling of personal data that may be of particular concern to individuals. The provision of sync technology which allows users to synchronise data with their mobile device could allow that mobile devices to be identified.

[8] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Google Apps for Education allows users to add a picture to their profile, thus identifying that individual visually across the system to other users. Guidance will be issued to user groups to ensure end users are aware of this service, and what the threat level would be.

The limited personal data used to provision accounts in the system does not include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings, financial data, particular data about vulnerable individuals, and data which can enable identity theft.

Q. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

A. No.

Q. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

A. No. The data help in Google Apps for Education will be focused on learning and teaching and the support of this activity.

Q. Will the project require you to contact individuals in ways which they may find intrusive?

A. No, users will be provided with access credentials via school contacts. In the event of an investigation, users will be contacted by a named individual within their school, normally a guidance teacher or member of the school senior management.

3.2 Consideration of responses to questions and recommendation

Given the limited scope of personal data held in the proposed system, the limited gathering of user data and limited risk of disclosure of personal data within the platform

Whilst the analysis of the screening process indicate that the answer to a number of the questions was a YES the CIO guidance stipulates that the answers to the questions need to be considered as a whole, in order to decide whether the overall impact, and the related risk, warrant investment in a full-scale PIA or in a smaller scale PIA.

The analysis of the above gathered information and engagements identified no requirement for Privacy Impact Assessment to be undertaken.