# Cloud Software Services for Schools

## Supplier self-certification statements with service and support commitments

| | |
|---|---|
| ***Supplier name*** | Google Ireland Limited |
| ***Address*** | Google Ireland Ltd<br>Gasworks Building<br>Barrow Street<br>Dublin 4<br>Ireland |
| ***Contact name*** | For queries relating to an existing Google Apps for Education account please use Google's standard support service, at http://contact.googleapps.com/<br>For queries related to this checklist, please contact:<br>Adam Stewart, Regional Manager - UK, Google Education |
| ***Contact email*** | ukdfe-questions@googlegroups.com |
| ***Contact telephone*** | +44 (0) 7919113421 |

# Contents

## Introduction

When entering into an agreement with a “cloud” service provider, every school/data controller has to be satisfied that the relevant service provider is carrying out its data processing as per their requirements (ensuring compliance with the Data Protection Act (DPA) by the data controller and also the data processor by default).

It is the responsibility of every school to ensure compliance with the DPA. This document is meant to act as an aid to that decision-making process by presenting some key questions and answers that should be sought from any potential cloud service provider.

The questions answered in sections 3 to 9 below will give a good indication as to the quality of a service provider’s data handling processes, although schools will still need to make their own judgement as to whether any provider fully meets DPA requirements.

The school/data controller should communicate its particular data handling requirements to the cloud provider (and each school could be different in its interpretation of what measures, procedures or policy best meet their DPA requirements), and confirm these by way of contract. The best way to set that out is to also put in place a data processing agreement with your chosen provider.

The principles of the DPA are summarised by the Information Commissioner’s Office at:

http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles

## 1. Supplier commitments

In order that schools can be confident regarding the accuracy of the self-certification statements made in respect of the Google cloud service, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields

- that their self-certification responses have been independently verified for completeness and accuracy by Liz Sproat who is a senior company official
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the Department is of the view that any element or elements of a cloud service provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

## 2. Using the Supplier Responses

When reviewing supplier responses and statements, schools will also wish to consider aspects of data security beyond the supplier-related issues raised in the questions. These include:

- how the school chooses to use the provided cloud service
- the nature, types and sensitivity of data the school chooses to place in the cloud service
- the extent to which the school adapts its own policies (such as acceptable use, homeworking, Bring Your Own Device (BYOD) and staff training to ensure that the way staff and students use the service is consistent with DPA guidance. Please refer to the Information Commissioner's Office (ICO) BYOD guidance: http://ico.org.uk/for_organisations/data_protection/topic_guides/online/byod
- the wider policies and practices the school has in place to ensure that the use of cloud services by their staff and students remains DPA compliant, Please refer to the ICO guidance on cloud computing: http://ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx
- the use of robust, strong, frequently changed authentication passwords and encryption keys, policies on BYOD / homeworking / acceptable use

to ensure that school data is accessed securely when either on or off the premises

- The security of the infrastructure that the school uses to access the supplier's cloud service including network and endpoint security.

The purpose of this particular document is to focus upon some key areas that schools should consider when moving services to cloud providers. Although it is designed to cover the most important aspects of data security, the checklist should not be viewed as a comprehensive guide to the DPA.

The self-certification checklist consists of a range of questions each of which comprises three elements:

- the checklist question
- the checklist self-certification response colour
- the evidence the supplier will use to indicate the basis for their response

For ease of reference, the supplier responses have been categorised as follows:

| | |
|---|---|
| Where a supplier is able to confirm that their service **fully meets** the issue identified in a specific checklist question (in a manner compliant with the obligations of the Data Protection Act where relevant), the appropriate self-certification colour for that question is GREEN. | |
| Where a supplier is **not able** to confirm that their service fully meets the issue identified in a specific checklist question (in a manner compliant with the obligations of the Data Protection Act where relevant), the appropriate self-certification colour for that question is AMBER. (*It should be made clear that a single "Amber" response is not necessarily a negative, and that any associated clarification should also be considered).* | |
| Where a supplier is able to confirm that a specific checklist question **does not apply** to their particular service the appropriate self-certification code for that question is **BLACK**. | |

There is space provided within the supplier response for links to relevant further information and clarification links.

Schools are invited to use the checklist to support their assessment of the extent to which the cloud services from a particular supplier meet their educational, technical and commercial needs in a DPA-compliant manner.

Schools should make a decision on the selection of a supplier based on an overall assessment of the extent to which their product meets the needs of the school, the overall level of risk and the nature and extent of support available from the supplier.

## 3. Supplier Response - Overarching Legal Requirements

Schools are required to ensure that all cloud services used enable them to meet their legal obligations under the DPA. To assist schools in that assessment, Google confirms the position to be as follows:

| Question | Supplier Response Code | Response Statement with Supporting Evidence (where applicable) |
|---|---|---|
| Q 3.1 – Does your standard contract for the supply of cloud services to UK schools fully comply with the DPA? | | Yes, we believe that our standard contract allows a UK school to meet the requirements applicable to it as a data controller under the UK Data Protection Act. In addition to our standard contract, we also offer all schools the option to amend the standard contract with our Data Processing Amendment. This Data Processing Amendment gives schools an additional means of meeting the requirements of the European Commission's Data Protection Directive for transfers of data to third countries. Google Apps administrators may opt in to the Data Processing Amendment by visiting the Google Apps Admin Console. From there, click Company Profile and then choose the Profile tab to navigate to the amendments listed under Security and Privacy Additional Terms. |
| Q 3.2 – If your standard | | n/a |

| | | |
|---|---|---|
| contract does not fully comply with the DPA, do you offer additional commitments to UK schools to help ensure such compliance? | | |
| Q 3.3 – Is your contract with UK customers enforceable both in the UK and in the country in which your company is registered? | | Yes, we offer customers a contract that is governed by English law and subject to the jurisdiction of the English courts. Our contract is viewable at this link: goo.gl/QPIZGy |
| Q 3.4 – Do your services ensure that schools are able to comply with their obligations with regard to the exercise of data subjects' rights? | | Users have access to their own information from within the services. In addition, Google provides the administrators of Google Apps accounts with tools which may assist customers with accessing data. These tools enable schools to exercise data subjects' rights within their Google Apps account. |

## 4. Supplier Response - Data Processing Obligations

The Data Protection Act (DPA) relates to personal data that is processed and is likely to be relevant to most of the operations that comprise a cloud computing service. This includes simple storage of data, the obtaining and handling of information, operations such as adaptation, organisation, retrieval and disclosure of data, through to erasure or destruction.

Schools, as data controllers, have a responsibility to ensure that the processing of all personal data complies with the DPA and this includes any processing carried out on their behalf by a cloud service provider.

To assist schools in understanding whether the cloud service being provided by [Supplier Name] is likely to comply with the DPA in relation to data processing, Google has responded as follows:

| Question | Supplier Response Code | Response Statement with Supporting Evidence (where applicable) |
|---|---|---|
| Q 4.1 – Taking account of the UK Information Commissioner's Office (ICO) guidance on Data Controllers and Data Processors, when providing the service, do you act at any time as a data controller in respect of the data processed as part of this service? | | No, Google does not act as the data controller. Customer shall be the data controller and Google shall be a data processor. |
| Q 4.2 – Where you act as a data processor does your contract ensure that you will only act on the instructions of the data controller? | | Yes, Google only acts according to the instructions of the data controller as provided in the contract. |
| Q 4.3 – Does your contract document the security measures that you implement to enable a school to ensure compliance with the DPA's security obligations? | | Yes, through its Data Processing Amendment to Google Apps Enterprise Agreement. |
| Q 4.4 – Is the processing of personal data or metadata limited to that necessary to deliver [or improve] the service? | | Google will only process customer data in accordance with the customer agreement and will not process Customer Data for any other purpose. For clarity, and notwithstanding any other term in the Agreement, Google will not serve Advertising in the Services or use Customer Data for Advertising purposes. |
| Q 4.5 – Where your contract does not cover every aspect of data processing, are you prepared to enter into a | | Google provides customers with a 'Data Processing Amendment to Google Apps Enterprise Agreement' to cover aspects of data processing not otherwise addressed directly in the |

| | | |
|---|---|---|
| separate data-processing agreement with your cloud services customer? | | Customer Agreement. |

## 5. Supplier Response - Data Confidentiality

When choosing a cloud service provider, schools must select a data processor providing sufficient guarantees about the technical and organisational security measures governing the processing to be carried out, and must take reasonable steps to ensure compliance with those measures.

The cloud customer should therefore review the guarantees of confidentiality that the cloud provider can commit to. To assist in understanding if the service being provided by Google is likely to comply with UK law in relation to data confidentiality Google has responded as follows:

| Question | Supplier Response Code | Response Statement with Supporting Evidence (where applicable) |
|---|---|---|
| Q 5.1 – Do you prohibit personal data or metadata being shared across other services that you as a supplier do or may offer? | | Google will process Customer Data in accordance with Customer's Instructions and will not process Customer Data for any other purpose. Customer instructs Google to process Customer Data to: (i) provide the Services (which may include the detection, prevention and resolution of security and technical issues) and (ii) respond to customer support requests. |
| Q 5.2 – Do you prohibit personal data or metadata being shared with third parties? | | Google's view is that requests for enterprise user data should be handled by the enterprise customers directly, and not Google. The customer is in the best position to make decisions about disclosure and evaluate options. Accordingly, when possible and legal to do so, we notify affected customers about requests for user data that may affect them and direct requesting parties to the customers. |

| | | |
|---|---|---|
| Q 5.3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts? | | Yes, login is encrypted via HTTPS (SSL) and you have the ability to enable 2-step authentication (http://goo.gl/o33Kf8)<br>at no additional cost. More information can also be found in our Security White Paper (http://goo.gl/3IQqnW). |
| Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts? | | Administrators can manage users' security settings to enforce 2-step authentication (http://goo.gl/o33Kf8) and password strength, and to revoke any application-specific passwords (http://goo.gl/IVDVTx) that have been granted access to the user's account. These steps can greatly reduce the risk of unauthorized access if a user's password is compromised. |
| Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data? | | Yes, Google's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process personal data. Google employs a centralised access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. |

*Questions 6.6 to 6.9 address the supplier approach to data encryption. The ICO guidance on encryption is as follows:*

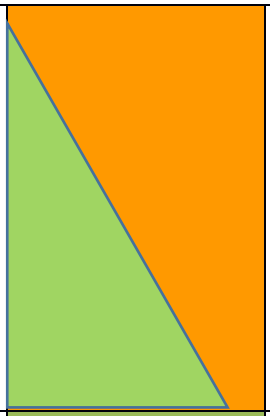
*There have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued.*

*The ICO recommends that portable and mobile devices, including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.*

*Personal information which is stored, transmitted or processed in information, communication and technical infrastructures, should also be managed and protected in accordance with the organization's security policy and using best practice methodologies such as using the International Standard 27001. Further information can be found at https://www.getsafeonline.org/*

*There are a number of different commercial options available to protect stored information on mobile and static devices and in transmission, such as across the internet.*

| | | |
|---|---|---|
| Q 5.6 – Does your cloud service insist that communications with access devices are encrypted? | | Yes it is possible to force users to access Google Apps core services via SSL, when you enable SSL (goo.gl/SIfCUH). In order to enable SSL, log into your Google Apps Admin Console (admin.google.com). Click on Security > Basic Settings. Under the General tab and in the SSL section, check the box next to Enable SSL. Click save changes. |

| | | |
|---|---|---|
| Q 5.7 – Does your cloud service ensure that data at rest is encrypted? |  | All data in transit is encrypted. As of June 25th, all files uploaded to Google Drive will be encrypted not only from your device to Google and in transit between Google data centers, but also at rest on Google servers.<br>Google is constantly working to extend and strengthen encryption across more services and links. |
| Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted? | | Google apps for education uses an encrypted HTTPS connection when you check or send email or Google applications. This means that no one can listen in on your messages as they go back and forth between you and Google's servers regardless of whether you're using public WiFi or logging in from your computer, phone or tablet.<br><br>In addition, every single email message you send or receive is encrypted while moving internally. This ensures that your messages are safe not only when they move between you and Gmail's servers, but also as they move between Google's data centres. |
| Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted? | | We provide this, but we cannot guarantee the practices of other companies providing cloud services. |
| Q 5.10 – Does your service provide defined timescales in respect of data destruction and deletion both during the contract and at contract end? | | Yes. Once Customer or End User deletes Customer Data (and such Customer Data cannot be recovered by the Customer or End User, such as from the "trash") Google will delete such Customer Data from its systems as soon as reasonably practicable and within a maximum period of 180 days. |

| | | |
|---|---|---|
| Q 5.11 – Does your service ensure that you use a secure deletion and erasure process which encompasses all copies of client/customer data? | | Yes |
| Q 5.12 – Does your service provide a mechanism free of charge whereby users can access a complete and secure copy of their data? | | Yes. Google aims to make it easy for our users to transfer their personal data in and out of Google's services, by building simple import and export functions. For more information, please see Google's Data Liberation Front (http://goo.gl/bD7tCW). From your account settings you can quickly and easily download data that you created in (or imported into) a number of Google products. Data is provided in a variety of open, portable formats. |

## 6. Supplier Response - Data Integrity

Data integrity has been defined as "the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission". To assist schools in understanding if the cloud service being provided by Google is likely to comply with the DPA in relation to data integrity Google has confirmed the position to be as follows:

| Question | Supplier Response Code | Response Statement with Supporting Evidence (where applicable) |
|---|---|---|
| Q 6.1 – Do you allow a trusted independent third party to conduct regular detailed security audits of the physical, technical and organisational aspects of your service? | | Yes. Google has been awarded an unqualified SSAE 16 and ISAE 3402 Type II audit opinion, and has earned ISO 27001 certification (http://goo.gl/CSwJe7).<br><br>The independent third party auditor verified that Google Apps has the following controls and protocols in place: |

| | | |
|---|---|---|
| | | • **Logical security:** Controls provide reasonable assurance that logical access to Google Apps production systems and data is restricted to authorized individuals<br>• **Data centre physical security:** Controls provide reasonable assurance that data centres that house Google Apps data and corporate offices are protected<br>• **Incident management and availability:** Controls provide reasonable assurance that Google Apps systems are redundant and incidents are properly reported, responded to, and recorded<br>• **Change management:** Controls provide reasonable assurance that development of and changes to Google Apps undergo testing and independent code review prior to release into production<br>• **Organization and administration:** Controls provide reasonable assurance that management provides the infrastructure and mechanisms to track and communicate initiatives within the company that impact Google Apps |
| Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers? | | Administrators of Google Apps for Education accounts may request the Statement on Standards for Attestation Engagements (SSAE) No. 16 Type II / International Standards for Assurance Engagements (ISAE) No. 3402 reports via the Google Apps support team. Customers may contact the support team via the “Support” link within their Admin Console. Prospective customers may request a copy of the audits via the contact email address. |

| | | |
|---|---|---|
| Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards? | | Our Google security audits are conducted following industry standards, such as ISO 27001 certification (http://goo.gl/CSwJe7) and SSAE 16/ ISAE 3402. |
| Q 6.4 – Are audit trails are in place enabling users to monitor who is accessing their data? | | Access to systems is logged to create an audit trail for accountability.<br>The Reports API lets Google Apps administrators customize usage reports across your whole account, for example, the number of logins in the past 30 days. And the API's activity reports let you understand user activities in specific Google Apps services such as the Admin console and Google Docs and Drive.- http://goo.gl/SvQWeP |
| Q 6.5 – Does your service ensure you could restore all customer data (without alteration) from a back-up if you suffered any data loss? | | Yes, Google's systems are designed to restore customer data (without alteration) from a back-up in the event of a data loss. |
| Q 6.6 – Does your service have a disaster recovery plan, and is information on this plan made available to current/prospective cloud service customers? | | Yes Google has a disaster recovery plan. In addition Google tests its Disaster Recovery (DR) on a regular basis, and publishes some of its thought leadership in the space for others to learn from e.g. goo.gl/AaKjz5<br><br>While some of the details of the DR plan are reported and audited in Google's SOC 2 and ISO 27001 report each year which is available to customers, the actual plan is confidential. However Google does commit to a 99.9% SLA with no scheduled downtime, and our track record has shown that we exceed this SLA. |

| | | |
|---|---|---|
| | | http://goo.gl/ZjsNmq<br>http://goo.gl/aB8YPj<br>http://goo.gl/gswVDY<br>http://goo.gl/XmB0iD<br><br>To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, Google frequently and thoroughly tests its DR plan.<br>Testing includes multiple components to minimize the risk of any single point of failure, including the following:<br>• Data replication and backup: To help ensure availability in the event of a disaster, Google Apps data is replicated to multiple systems within a data centre, and also replicated to a secondary data centre.<br>• Google operates a geographically distributed set of data centres that is designed to maintain service continuity in the event of a disaster or other incident in a single region. High-speed connections between the data centres help ensure swift failover. Management of the data centres is also distributed to provide location-independent around-the-clock coverage, and system administration.<br>In addition to the redundancy of data and regionally disparate data centres, Google also has a business continuity plan for its headquarters in Mountain View, CA. This plan accounts for major disasters, such as a seismic event or a public health crisis, and it assumes people and services may be unavailable for up to 30 days. This plan is designed to enable continued operations of our services for our customers.<br>Further information is available from the Google Enterprise Blog : http://goo.gl/YNp0Wo. |

## 7. Supplier Response - Service Availability

Service availability means ensuring timely and reliable access to personal data. One threat to availability in the cloud which is often outside the responsibility of the cloud service provider is the accidental loss of network connectivity between the client and the provider of service.

Data controllers should therefore check whether the cloud provider has adopted reasonable measures to cope with the risk of disruptions, such as backup internet network links, redundant storage and effective data backup mechanisms.

To assist schools in understanding if the service being provided by a particular company is likely to comply with the DPA in relation to service availability Google has confirmed as follows:

| Question | Supplier Response Code | Response Statement with Supporting Evidence (where applicable) |
|---|---|---|
| Q 7.1 – Can you confirm that you have sufficient capacity to ensure you can provide a resilient, reliable and accessible service at all times? | | The application and network architecture run by Google is designed for maximum reliability and uptime. Google's computing platform assumes ongoing hardware failure, and robust software fail-over withstands this disruption. All Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation. Data is replicated multiple times across Google's clustered active servers, so, in the case of a machine failure, data will still be accessible through another system.<br><br>Google offers a 99.9% uptime guarantee (http://goo.gl/09Nlwx) to its customers. With Google Apps, there is no planned downtime.<br>Rather than storing each user's data on a single machine or set of machines, we |

| | | |
|---|---|---|
| | | distribute all data—including our own—across many computers in different locations. We then chunk and replicate the data over multiple systems to avoid a single point of failure. We randomly name these data chunks as an extra measure of security, making them unreadable to the human eye.<br><br>While you work, our servers automatically back up your critical data. So when accidents happen—if your computer crashes or gets stolen—you can be up and running again in seconds. |
| Q 7.2 – Does your service offer guaranteed service levels? | | Yes, Google Apps for Education customers are guaranteed 99.9% uptime in their contract.<br><br>In 2013, Gmail was available 99.978% of the time, which averages to less than two hours of disruption for a user for the entire year. Our engineering experts work 24 hours a day, 7 days a week and are available immediately should an issue arise. We keep customers informed by posting updates on the Apps Status Dashboard (http://goo.gl/Fy4Jja) until the issue is fixed, and we always conduct a full analysis on the problem to prevent it from happening again. |
| Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met? | | Yes, During the Term of the applicable Google Apps Agreement, the Google Apps Covered Services web interface will be operational and available to Customer at least 99.9% of the time in any calendar month. If Google does not meet the Google Apps SLA, and if Customer meets its obligations under this Google Apps SLA, Customer will be eligible to receive Service Credits. See credits on the SLA site (http://goo.gl/09Nlwx). |

## 8. Supplier Response - Transfers beyond the European Economic Area (EEA)

The eighth principal of the DPA permits the transfer of personal data beyond the EEA when adequate arrangements are in place to ensure rights and freedoms of data subjects in relation to the processing of personal data.

The eighth principal of the DPA states:
“Personal data shall not be transferred to any country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data” Guidance on data transfers published by the ICO states:

“If you decide you need to transfer personal data outside the EEA, and the recipient is not in a country subject to a positive finding of adequacy by the Commission, nor signed up to the Safe Harbor Scheme, you will need to:
- conduct a risk assessment into whether the proposed transfer will provide an adequate level of protection for the rights of the data subjects; or
- if you do not find there is an adequate level of protection, put in place adequate safeguards to protect the rights of the data subjects, possibly using Model Contract Clauses or Binding Corporate Rules; or
- consider using one of the other statutory exceptions to the Eighth Principle restriction on international transfers of personal data.”

The European Commission has approved four sets of standard contractual clauses (known as model clauses) as providing an adequate level of protection where data is transferred outside the EEA.

If your service provider offers these model clauses in their entirety in their contract, you will not have to make your own assessment of adequacy. To assist schools in understanding if the cloud service being provided is likely to comply with the DPA in relation to permitted transfers of personal data beyond the EEA, Google has responded as follows:

| Question | Supplier Response Code | Response Statement with Supporting Evidence (where applicable) |
|---|---|---|
| Q 8.1 – In providing the service do you limit the transfer of personal data to countries within the EEA? | | In accordance with ICO guidance (goo.gl/ppoe4H) regarding the transfer of personal data outside of the EEA, Google offers both 1) participation in the US-EU (and Switzerland) Safe Harbor framework and 2) model contract clauses as means of meeting the adequacy and security requirements of the European Commission's Data Protection Directive, thus negating the need to limit the transfer of personal data outside the EEA. As such, Google does not limit the transfer of personal data outside the EEA. |
| Q 8.2 – If you transfer data outside the EEA do you explain to schools when (and under what circumstances) data will be transferred to these locations? | | Yes, this is explained in the Google Apps for Education Agreement: As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its Group Companies maintain facilities. |
| Q 8.3 – If you transfer data outside the EEA does your standard contract include the unmodified EU approved "model clauses" in respect of such transfers? | | Google offers a data processing amendment and the full text of EU-approved model clauses to customers as amendments to the standard contract. In conformity with clause 10 of the model clauses, Google adds a clause - provided strictly for business-related issues - involving each party's aggregate liability to the other. This provision does not modify or contradict the model clauses. Further, in conformity with guidance provided by the Article 29 Working Party Opinion 05/2012 on Cloud Computing, in its data processing amendment Google provides for independent third party audits of Google systems in lieu of direct customer audits. |

| | | |
|---|---|---|
| Q 8.4 – If you transfer data outside the EEA, (and do not offer the unmodified EU approved "model clauses", can you confirm that the requirements of the DPA are met in respect of the need for adequate protection for the rights and freedoms of data subjects in connection with the cross-border transfer and processing of their personal data? | | Google participates in the US-EU Safe Harbor Framework, as well as offering a data processing amendment and model contract clauses as an additional means of meeting the adequacy and security requirements of the European Commission's Data Protection Directive. |

## 9. Supplier Response - Use of Advertising

Recognising the particularly sensitive nature of the data likely to be processed in a cloud service aimed at schools, there is particular concern in relation to the use of advertising and the extent of data mining which providers of cloud-based services may adopt in relation to user data.

To assist schools in understanding if the cloud service provided by a particular company will involve serving advertisements or engaging in advertisement-related data mining or advertisement-related profiling activities, suppliers will be asked to indicate in respect of services to **pupil and staff users** as follows:

*ICO cloud computing guidance states that "In order to target advertisements the cloud provider will need access to the personal data of cloud users. A cloud provider may not process the personal data it processes for its own advertising purposes unless this has been authorised by the cloud customer and the cloud customer has explained this processing to cloud users. Individuals have a right to prevent their personal data being used for the purpose of direct marketing".*

*So a school would have to agree to the advertising and then would have a duty to explain to staff and pupils what personal data would be collected, how it will be used and by whom, and what control they have over the use of their data in this way.*

*As there are obvious difficulties with schools deciding if children are competent enough to understand any explanation of their data being used for advertising, and to understand and exercise their right to object, without parental involvement it would seem sensible to avoid this in solutions for schools, especially where children are concerned.*

| Question | Supplier Response Code | Response Statement with Supporting Evidence (where applicable) |
|---|---|---|
| Q 9.1 – In providing the cloud service, is the default position that you enter into a legally binding obligation not to serve advertisements to any | | Yes. |

| | | |
|---|---|---|
| pupil or staff users via your school cloud service? | | |
| Q 9.2 – In providing the cloud service, is the default position that you enter into a legally binding obligation not to conduct any advertisement-related data mining in respect of pupil or staff data or metadata? | | Yes. |
| Q 9.3 – In providing the cloud service, is the default position that you enter into a legally binding obligation never to use for any commercial purpose (or pass on to others) personal data or metadata in respect of pupil or staff users of your service? | | Under our Data Processing Amendment, Google will only process Customer Data in accordance with the customer agreement and will not process Customer Data for any other purpose. For clarity, and notwithstanding any other term in the Agreement, Google will not serve Advertising in the Services or use Customer Data for Advertising purposes. |

# Appendix 1: Availability and extent of support available to schools when using cloud software services.

## Table of Contents

# Section 1.0 Introduction

The Department for Education intends that schools who are considering the use of cloud based services should have easy access to information in relation to:

- Responsibilities in respect of Data Protection Act compliance. General guidance for schools can be found at http://ico.org.uk/for_organisations/sector_guides/education
- The general levels of security inherent in the solutions offered by many of cloud service providers as compared to what might apply to their current arrangements – this information is provided in the general guidance statements to be found at (hyperlink tba.gov)
- The data protection implications of using a particular supplier's cloud services – addressed through the self-certification process detailed in the associated checklist document found above
- The normal support mechanisms available in respect of routine administrative or technical support issues – this is addressed by inviting cloud service providers who are participating in the self-certification process to complete the statements summarising their routine support arrangements as above.
- **The additional support** that would be available in the unlikely event of some **serious data-related incident** related to the use by schools of cloud services – this is addressed by inviting cloud service suppliers to indicate how they would respond to a number of specific challenges that a school might face in the event of such a serious breach or failure.

**Section 2.0** of this document sets out the rationale underpinning the need for greater clarity in the event of some serious data-related event.

**Section 3.0** sets out those areas where specific supplier commitments on additional support are invited.

# Section 2.0 Managing Worst Case Scenarios

Whilst there is much to be gained from adopting a cloud service platform, it is only prudent that schools should, as part of their overall risk assessment, and prior to deploying a cloud service, understand (in the event of a data-protection related “worst case scenario”) the nature and extent of the support that would be forthcoming from a potential cloud service provider.

It is also clearly in the interests of cloud service providers themselves to work with schools to address the technical, business, reputational and legal issues which would flow from some such incident, and which resulted in for example:

- A significant data loss flowing from a breach of security associated with the provision of cloud service
- A breach of privacy whereby confidential data was released to a person or persons not authorised to receive it
- A serious disruption to the school’s business, educational or administrative processes

The key headings that cloud service providers are invited to respond against are set out in **Section 3**. When responding to the various issues set out in Section 3, cloud service providers should draft their response assuming that the intended audience is non-technical senior staff in schools.

Suppliers may, of course, make reference to supporting management or technical documents but the response provided here should go beyond referring to “terms of service” and should set out clearly and simply what additional support could be expected in the event of a data protection-related “worst case scenario”.

# Section 3.0 Key Support Areas

The key areas that cloud service providers are invited to respond against in respect of a serious incident are:

- Solution configuration
- Communicating serious breaches
- Supplier responsibilities
- Restoring data
- Managing media attention
- Engaging with the child protection agencies
- Engaging with the wider school community

These are minimum suggested areas and suppliers are free to set out additional support capabilities which could be used in the event of a serious incident and which they feel will engender confidence in schools and differentiate the supplier in this competitive and growing marketplace.

## 3.1 ADDRESSING SERIOUS INCIDENTS

Cloud service providers should as a minimum clarify in this area of their response:

- How schools should log any serious issues regarding the use of the service, providing as a minimum a UK phone number and support email address. It is better to provide an indication of the individuals or roles that should be the first point of contact – for example "you should also contact our Head of Security J.Smyth@company.com phone number +44 (0) 12345678 who will also make sure our education /public sector team at [xxx] is contacted". It would also be useful to cover all time scenarios – out of hours, weekends etc.
- The nature of the support that might be available – for example, is it limited to phone and/or email or are there circumstances when on-site support might be required.
- How the cloud service provider might work with schools to address the consequences of the serious incident
- Whether in addition to contacting the incident support centre there are other resources that could be made available – for example via online tools and resources, a partner ecosystem, a local public sector or education support team or identified escalation routes within the company that should be utilised.

*Google provides 24/7 support to our Education customers. If you experience a serious issue, the first step is to call or email the support team. Domain administrators can generate a PIN number via their Control Panel. On calling the support centre on* 0800-169-0455*, customers will be asked to enter their PIN number. Administrators may also file a ticket via our online portal:*
http://contact.googleapps.com/

*Often, users may find an answer more quickly via online resources which are also available to all our users:*

- *Apps service status:* Apps Status Dashboard (http://goo.gl/Fy4Jja) *and* Known Issues (http://goo.gl/LCIXvD)
- *Deployment:* Planning and training resources (http://goo.gl/TBpPgD)
- *Documentation:* Admin Help Centre (http://goo.gl/FHzIqb)
- *Forums:* Administrators (http://goo.gl/ghIC61) and Developers (http://goo.gl/T82B6K)
- *Feature & product launches:* What's new with Google Apps (http://goo.gl/3N2mMw)
- *Technical support:* Contact Google Technical support (http://contact.googleapps.com/)
- *Troubleshooting:* Troubleshooting resources (http://goo.gl/KJN4Zw)
- *User Help Centres:* Gmail (http://goo.gl/8MsE4p) **|** Calendar (http://goo.gl/DzGz70) **|** Drive (http://goo.gl/axpIZD) **|** Sites (http://goo.gl/w9xAZa) **|** Mobile (http://goo.gl/EI6qgZ) **|** More… (http://goo.gl/9y4nwb)

*Support from Google is via phone, email and online help centre support.*

*For catastrophic events, the first point of call will always be the support team who will be best placed to assist. The Google UK press office is also manned 24 hours a day, 7 days a week and can easily be reached by emailing press-uk@google.com. The Google press office will be able to help any school with advice on handling media inquiries resulting from a serious event.*

### 3.2 SUPPLIER RESPONSIBILITIES

In this section cloud service providers should, as a minimum, set out (in language aimed at school managers), their responsibilities when working with schools to address the implications of a serious incident.

In addition, cloud service providers should describe what practical assistance they would be able to offer which *goes beyond* the "contractual minimum" as set out in their terms and conditions.

Google has implemented a robust disaster recovery programme at each data centre. It is important to first note the processes Google has put in place to avoid a disaster scenario impacting our customers:

The Google disaster recovery programme includes multiple components to minimize the risk of any single point of failure, including the following:

- Data replication and backup: To help ensure availability in the event of a disaster, Google Apps data is replicated to multiple systems within a data centre, and also replicated to a secondary data centre
- Google operates a geographically distributed set of data centres that is designed to maintain service continuity in the event of a disaster or other incident in a single region. High-speed connections between the data centres help ensure swift failover. Management of the data centres is also distributed to provide location-independent, around-the-clock coverage, and system administration.

In addition to the redundancy of data and regionally disparate data centres, Google also has a business continuity plan for its headquarters in Mountain View, CA. This plan accounts for major disasters, such as a seismic event or a public health crisis, and it assumes people and services may be unavailable for up to 30 days. This plan is designed to enable continued operations of our services for our customers. We conduct regular testing of our Disaster Recovery Plan.
Further information is available from the Google Enterprise blog (http://goo.gl/YNp0Wo).

Google's systems are designed to restore customer data (without alteration) from a back-up in the event of a data loss.

### 3.3 SOLUTION CONFIGURATION.

Whilst virtually all cloud service providers have detailed technical advice on how their systems should be configured, this section of the supplier response should set out the general principles which school management should expect to see implemented to ensure maximum security of their cloud implementation.

This might cover for example:

- The need for correct configuration of access devices
- The use of additional backup / data synchronisation arrangements for sensitive or business critical data
- Configuration options or additional services that provide greater level of security than is available in your free offering
- Sample password policies in relation to the age and ability of the users of their service
- Policies in respect of helpdesk and security staff access to client data

***Deployment***

- Domain Best Practice (http://goo.gl/V3mzIU) *on how to setup your Google Apps domain*
- Google Apps for Education Deployment Guide (http://goo.gl/RgXgA2) *to ensure a smooth transition for your technology team, your teachers, and your students*
- Google Apps Technical Transition Guide Technical Transition Guide (http://goo.gl/LIxIOR) - *a full in-depth guide for all your technical questions.*

***Training***

- Education Training Website (http://goo.gl/XpYaXS) *that includes information on* administering (http://goo.gl/DFOFbd) *Google apps and basic product training*
- In depth product training (http://goo.gl/31ZilA) *for all core products*
- Education Change Management Guide (http://goo.gl/vnY4tz) *which includes strategy and information on everything to do with change management.*

***Support***

- *Google provides 24/7 support to our Education customers. If you experience a serious issue, the first step is to call or email the support team. Domain administrators can generate a PIN number via their Control Panel. On calling the support centre on* 0800-169-0455*, customers will be asked to enter their PIN number. Administrators may also file a ticket via our online portal:* http://contact.googleapps.com/
- *All other users will have access to the Google Apps Help Centre (http://goo.gl/FHzIqb).*

*Your school assumes the responsibility for complying with child privacy protection policies. Per the Google Apps Education Edition Agreement, any school administering Google Apps Education Edition acknowledges and agrees that it is solely responsible for compliance including, but not limited to, obtaining parental consent concerning collection of students' personal information used in connection with the provisioning and use of the Services by the Customer and End Users. Parental consent and notification could take place in form of a permission slip granting use of Google Apps and/or other technology services at the school.*

*Most schools already have an internet policy in place that requires parental permission for internet access at school etc. If a school moves to Google Apps, these permission forms should specifically reference the school's use of Apps for Education.*

*We would also recommend the school's IT team to investigate the security policies, for example, walled garden (http://goo.gl/g9uO2E), turning on/off services by Org Unit (http://goo.gl/RABPkl), 2-step verification (http://goo.gl/o33Kf8) and objectionable content filters (http://goo.gl/i0tlKo), and make sure that they are*

*familiar with the general security features (http://goo.gl/r05tld) of Apps. Once the school has investigated all the child protection possibilities then they should be able to answer any parent's questions and/or create their own information sites like two schools have done here, (http://goo.gl/DZGXPe) and here, (http://goo.gl/Sa6U8j) which gives information to address the concerns of parents and the steps that they are taking to protect the children using Google Apps within the school.*

*See some of Google's suggested template letters for parents,* (http://goo.gl/VmzUyA).

*Examples of Google promoting online safety: Good to Know programme* (http://goo.gl/UyvJRy).

### 3.4 RESTORING DATA

Where a serious event had occurred which resulted in the loss of data by a school, cloud service, providers should set out what steps they would take to work with the school to recover and restore to the maximum extent possible the data which has been lost (or corrupted). This section should also include indicative timescales.

Customers should first contact the support team for initial support and to log their issue. The support team can be reached on 0800-169-0455

and is available to all Google Apps administrators. Administrators may also file a ticket via our online portal: http://contact.googleapps.com/

Google's systems are designed to restore customer data (without alteration) from a back-up in the event of a data loss.

### 3.5 MANAGING MEDIA ATTENTION

Where a serious event had occurred which resulted in significant media attention falling on the school, suppliers should indicate the steps they would take as a responsible service provider to work with the school in managing the media attention.

The Google UK press office is manned 24 hours a day, 7 days a week and can easily be reached by e mailing press-uk@google.com. The Google press office will be able to help any school with advice on handling media inquiries resulting from a serious event.

### 3.6 ENGAGING WITH CHILD SUPPORT AGENCIES

Where a serious event had resulted in issues being raised that related to child protection – for example the loss of sensitive pupil data, the cloud service provider should indicate what it would do to assist the school in engaging with the relevant child protection agencies, over and above the contractual minimum.

1. Customers should first contact the Google Apps support team for initial support and to log their issue.
2. Google believes that it is the responsibility of the Data Controller (the school) to inform the relevant authorities should their systems be hacked and pupil data is leaked. However, our Google Apps support team will be on standby to provide as much technical support as possible. Administrators can also manage users' security settings to enforce 2-step authentication (http://goo.gl/o33Kf8) and password strength, and to revoke any application-specific passwords (http://goo.gl/lVDVTx) that have been granted access to the user's account. These steps can greatly reduce the risk of unauthorized access if a user's password is compromised.
3. The UK Google press office can be contacted for advice on handling any media fall-out from any data controller leak.
4. In the unlikely event that Google's wider systems are hacked and personal data is leaked or lost then Google will be responsible for a) contacting the Data Protection Agency to inform them of the leak and b) contacting all affected schools and providing them with guidance on defeating the hack and making their systems secure once again.

### 3.7 ENGAGING WITH THE WIDER SCHOOL COMMUNITY

Where a serious incident had resulted in issues being raised that related to the wider school community – for example parents, the local authority, the curriculum or examination bodies or the Information Commissioners Office, the cloud service provider should indicate what it would do to assist the school in engaging with the relevant organisation to address the implications of the serious incident. Again, this should describe available support over and above the contractual minimum.

1. Customers should first contact the Google Apps support team for initial support and to log their issue
2. In the unlikely event that Google's wider systems are hacked and personal data is leaked or lost then Google's first priority will be to recover the leaked or lost data.
3. In the even more unlikely event that Google is not able to recover any of the leaked or lost data then Google will take responsibility for alerting any relevant

authority (such as an examination board) and provide the necessary evidence that something untoward has occurred and the fault was not that of the pupil or school.