Department for Education

Cloud (educational apps) software services and the Data Protection Act

Departmental advice for local authorities, school leaders, school staff and governing bodies

October 2014

Contents

1. Summary

About this departmental advice

This is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based “cloud” service provision.

This advice is underpinned by a supplier self-certification scheme enabling providers to confirm their compliance with the key principles and requirements of the DPA, to provide useful additional advice and to suggest how cloud software solutions can best be configured by a school.

Important disclaimer

The particular focus of this document is to help schools by reducing the burden and complexity associated with understanding whether a particular supplier’s cloud service claims to meet the relevant UK legal requirements in respect of data protection. This guidance is not intended to relieve schools of any legal responsibility under the Data Protection Act and any associated legislation.

All schools, as independent public bodies, are directly responsible under the DPA for the collation, retention, storage and security of all information they produce and hold. This includes educational records, headteacher’s reports and any other personal information of individuals - pupils, staff and parents. As such, many schools may wish to consult their legal advisers and develop a data retention policy in accordance with the DPA.

Schools should also consider:

- obtaining their own data protection and/or legal advice;
- formulating their own data protection or data handling policies;
- making sure that staff understand or follow policy when handling personal data.

General data protection advice for schools can be found on the ICO website.

Expiry or review date

This advice will be reviewed on an annual basis or in light of significant changes to data protection responsibilities.

Who is this advice for?

This advice is for:

- School leaders, school staff and governing bodies in all maintained schools, academies and free schools
- Local authorities

How should this advice be used?

This document is designed to provide a straightforward overview of the type of obligations that schools have in respect of data security, especially when considering moving services to “the cloud”.

As well as the general guidance provided in this document, there are also links provided to supplier checklist and service provision documents that enable a comparison to be made between a variety of providers. These are intended purely as an aid to decision-making and should not be viewed in isolation. (See Section 6.)

Section 7 provides more useful links that give detailed insight into the Data Protection Act and all the responsibilities that attach.

Main points

The Data Protection Act 1998 (DPA) sets out the legal framework in relation to the processing of personal data. Compliance with the DPA is enforced and overseen by the Information Commissioners Office (ICO), the independent authority established to uphold information rights in the public interest and promote openness by public bodies and data privacy for individuals.

Anyone who processes personal information must comply with the eight principles of the DPA, which make sure that personal information is:

- fairly and lawfully processed
- processed for specific purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary
- processed in line with individuals’ rights
- secure

- not transferred to other countries without adequate protection

When considering data protection alongside potential take-up of cloud solutions, schools should be aware of the various challenges and responsibilities in respect of personal data that still remain (or indeed are created by this type of processing) . Whilst school and childrens' data may be stored and controlled in the cloud by a supplier, responsibility for all areas of data protection compliance still rests with the particular school.

Information Commissioner's Office

The Information Commissioner's Office (ICO) recognises this situation and recently provided the supportive statement below in respect of this DfE initiative:

"Schools are often responsible for very sensitive information about children, and it's crucial they handle that data in line with the law. We welcome this support being provided around one of the more technical aspects of that law, and are happy it sits well besides our own guidance on cloud computing. We'd hope too that it will encourage schools to ensure they are making informed decisions more generally around how they handle personal data."

(Information Commissioner's Office - November 2013)

2. Data protection obligations

Schools who have a comprehensive knowledge and understanding of data protection requirements and how these are impacted by the storing of data in the ”cloud” should already be able to make clear and informed choices regarding their cloud service provider.

It is recognised, however, that the majority of schools have only an outline knowledge of how data protection should be approached in a “cloud” environment. This document and the associated checklist are designed to enable a quick and meaningful comparison between the services offered by the key providers.

The aim of this particular document is to highlight key areas of concern and to demonstrate the degree to which various suppliers comply with the law and its main provisions.

These areas have been highlighted within this document and suppliers have been asked to confirm their position via a number of clear statements that can be found via the link in Section 6. Schools wishing to compare cloud service providers are therefore recommended to review these statements in order to fully understand the respective supplier positions regarding data protection and legal compliance.

Privacy Impact Assessment

Schools may also wish to consider whether carrying out a Privacy Impact Assessment (PIA) would be appropriate to identify and minimise the privacy risks of new projects, systems and solutions when deciding whether to implement them. The ICO has a new code of practice on PIAs.

3. Key obligations for schools

The key areas that schools need to address under the Data Protection Act (DPA) are:

Overarching legal requirements

Schools should ensure that their personal data is processed in compliance with the DPA.

Data processing

Schools, as data controllers, have a responsibility to ensure that the processing carried out by their cloud service provider complies with the DPA. The best way to do this is to have a contract and a data processing agreement in place.

Data confidentiality

When choosing a cloud service provider schools should 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.

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 a particular company is likely to comply with the DPA in relation to data integrity suppliers will be asked to confirm their compliance.

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 service provider. Data controllers should therefore check whether they have adopted reasonable measures to cope with the risk of disruptions such as backup internet network links. Data controllers should also assess the level of risk and whether the school is prepared to accept that risk.

Data transfers beyond the European Economic Area (EEA)

To assist schools in understanding whether the cloud service being provided by a particular company is likely to comply with the DPA in relation to permitted transfers of personal data beyond the EEA, suppliers will be asked to confirm they meet the requirements of the DPA.

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 being 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 confirm their policy.

ICO guidance states:

> "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. Remember that individuals have a right to prevent their personal data being used for the purpose of direct marketing".

So the 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.

4. Self-certification and how it works

Supplier responsibilities

In order that schools can be confident regarding the accuracy of the self-certification statements made by cloud service suppliers, those suppliers entering into the self-certification process are required to agree:

- that their self-certification checklist has been fully and accurately completed by a person or persons who are competent in the relevant fields
- that their self-certification checklist has been independently verified for completeness and accuracy by a named senior official of the cloud service provider
- that they will update their self-certification checklist 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 the cloud service provider will provide any additional information or clarification sought by the Department 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 checklist requires independent verification, the cloud service provider will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Department for Education role

The Department is facilitating this checklist procedure and will make the completed self-certification statement from a cloud service provider available via its website when:

- it is satisfied that the self-certification checklist is accurate and complete
- the self-certification checklist is supported by a declaration of accuracy and completeness by a named senior official of the cloud service provider
- there are no outstanding issues of clarification or verification
- the cloud service provider has not withdrawn from the self-certification scheme

The cloud service provider may withdraw from the self-certification process at any time.

The Department may end the self-certification process and cease to publish the self-certification statements at any time.

Important note regarding choice of supplier

It is important to understand that the Department is not endorsing the products or services made available by any particular cloud service provider and has not itself quality assured any supplier products or services as part of this exercise.

Selection of supplier should be based on a number of key criteria (including data protection practices and service levels) and is entirely a matter for the particular school.

5. Using the checklists

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:

Supplier response	Category
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. *(NB It should not always be assumed that an Amber response is a negative, and there is space provided in the checklist response for clarification where appropriate)*	
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.

Naturally there are a range of criteria that suppliers need to satisfy on behalf of schools before being appointed and DPA compliance is just one of these.

6. Supplier checklists

The current supplier's checklist statements can be found here. Please click on the relevant supplier hyperlink:

- Google
- Microsoft
- Other suppliers will be added as they complete responses

In addition to completing the supplier framework in relation to the DPA implications of using their service, suppliers have also undertaken to provide additional clarity in respect of:

- The technical configuration of their service – *available via supplier specific link above*
- The support infrastructure they have in place to assist UK schools in the event of some serious and unforeseen issue in relation to the use of their cloud service – *available via supplier specific link above*

7. Accessing further information

The ICO has issued a number of useful documents which are relevant to the use of cloud computing services by schools. They include:

- ICO Data Protection principles
- ICO guide to Privacy Impact Assessments
- ICO Guidance on the use of Cloud Computing
- ICO 2012 report on the Data Protection Act and schools
- ICO Guidance on assessing the adequacy of International Data Transfers
- ICO Guidance on Bring Your Own Device (BYOD)

Should you require any further assistance regarding the information contained within this document, please contact: schools.ictsupport@education.gsi.gov.uk.

Department for Education

About this publication:
enquiries www.education.gov.uk/contactus
download www.gov.uk/government/publications

Reference: DFE-00631-2014

Follow us on Twitter:
@educationgovuk

Like us on Facebook:
facebook.com/educationgovuk