

# Cloud Software Services for Schools

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

Please insert supplier details below

<b>Supplier name</b>	EducationCity Ltd
<b>Address</b>	Units 8/9 Saddlers Court, Oakham, Rutland, LE15 7GH
<b>Contact name</b>	Graham Lyden – Data Controller
<b>Contact email</b>	<a href="mailto:grahamlyden@educationcity.com">grahamlyden@educationcity.com</a>
<b>Contact telephone</b>	01572 725 080

# Contents

1. Supplier Commitments .....	3
2. Using the Supplier Responses .....	3
3. Supplier Response - Overarching Legal Requirements .....	6
4. Supplier Response - Data Processing Obligations .....	7
5. Supplier Response - Data Confidentiality .....	9
6. Supplier Response - Data Integrity .....	14
7. Supplier Response - Service Availability .....	15
8. Supplier Response - Transfers beyond the EEA .....	16
9. Supplier Response - Use of Advertising .....	19

## 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](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 EducationCity.com 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 the Managing Director 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



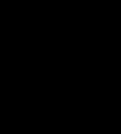
- the nature, types and sensitivity of data the school chooses to place in the cloud service
- the extent to which the school adapts its own policies (such as acceptable use, homeworking, Bring Your Own Device (BYOD) and staff training to ensure that the way staff and students use the service is consistent 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](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,
- 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 <b>fully meets</b> 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 <b>GREEN</b> .	
Where a supplier is <b>not able</b> 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 <b>AMBER</b> . <i>(It should be made clear that a single “Amber” response is not necessarily a negative, and that any associated clarification should also be considered).</i>	
Where a supplier is able to confirm that a specific checklist question <b>does not apply</b> to their particular service the appropriate self-certification code for that question is <b>BLACK</b> .	

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, EducationCity confirms the position to be as follows for its web-based educational software service, fuller details of which can be found at:

<http://www.educationcity.com/uk/search/node/Data%20Protection%20Agreement>

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?		<p>We meet all the requirements of the 8 Data Processing Principles contained within the Data Processing Act.</p> <p>Further information can be found here:  <a href="http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy">http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy</a></p>
Q 3.2 – If your standard contract does not fully comply with the DPA, do you offer additional commitments to UK schools to help ensure such compliance?		N/A

<p>Q 3.3 – Is your contract with UK customers enforceable both in the UK and in the country in which your company is registered?</p>		<p>Yes. We offer customers a contract governed by English law and subject to the jurisdiction of the English Courts.</p> <p>EducationCity Ltd is registered with Companies House in the UK, registration number: 03343749</p>
<p>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?</p>		<p>Yes.</p> <p>See under 'Access to information':</p> <p><a href="http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy">http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy</a></p>

#### 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 EducationCity is likely to comply with the DPA in relation to data processing, EducationCity Ltd has responded as follows:

Question	Supplier Response Code	Response Statement with Supporting Evidence (where applicable)
<p>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?</p>		<p>EducationCity does not act as the data controller in respect of the cloud service but does act as data controller of customer account information (ie: billing and administrator information).</p>
<p>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?</p>		<p>See: <a href="http://www.educationcity.com/uk/terms-conditions-schools">http://www.educationcity.com/uk/terms-conditions-schools</a> Section 6 Customer Data – “You continue to own all right, title and interest to all of your own customer data”.</p> <p>See also: <a href="http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy">http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy</a> Sharing Data - “EducationCity will not share data with 3<sup>rd</sup> parties unless explicit instruction is given by the school in question.”</p>
<p>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?</p>		<p>Yes All remote access via the EducationCity web application is conducted over HTTPS, an encrypted web link secured using Secure Sockets Layer (SSL).</p>



Q 4.4 – Is the processing of personal data or metadata limited to that necessary to deliver [or improve] the service?		Yes, the processing of personal data or metadata is only ever done for the purpose of delivering the service.
Q 4.5 – Where your contract does not cover every aspect of data processing, are you prepared to enter into a separate data-processing agreement with your cloud services customer?		N/A EducationCity’s contract covers all relevant aspects of data processing.

## 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 EducationCity is likely to comply with UK law in relation to data confidentiality EducationCity Ltd 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?		Yes. EducationCity will process customer data in accordance with customers' instructions and will not process customer data for any other reason.
Q 5.2 – Do you prohibit personal data or metadata being shared with third parties?		Yes, no customer data is shared with anyone beyond the organisation unless by express instruction from the head teacher or administrator in order to link to another service provider such as a VLE.
Q 5.3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts?		<p>Yes, protected by individual logins at three levels of pre-defined access abilities as determined at school-level. All provided over encrypted (SSL) connections.</p> <p>In addition, our off-site database backups from the UK data centre are shipped over an SSH encrypted connection to our UK server. Remote access to the servers is locked down to our office and data centre external IP addresses and requires an SSH key or the root password.</p>

<p>Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?</p>		<p>Yes, (see 5.3 above). Automated logouts after periods of inactivity as defined within our Privacy and Data Policy, under the section entitled ‘In Product Data Collection and Use’: <a href="http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy">http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy</a></p>
<p>Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?</p>		<p>Yes, within the company, access is controlled through the use of authorised and documented system access request notifications.</p>
<p><i>Questions 5.6 to 5.9 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.</i></p> <p><i>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.</i></p> <p><i>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 <a href="https://www.getsafeonline.org/">https://www.getsafeonline.org/</a></i></p>		

*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.*

<p>Q 5.6 – Does your cloud service insist that communications with access devices are encrypted?</p>		<p>Yes – Secure remote access is deployed for all company devices, which are also encrypted and password protected. Our product can only be accessed via SSL using secure https routes.</p>
<p>Q 5.7 – Does your cloud service ensure that data at rest is encrypted?</p>		<p>Passwords are encrypted at rest using a 2-way authenticated 256bit AES encryption. All other data at rest is not fully encrypted but the servers that it rests in are kept in a highly secure environment, in a locked cage within the data centre, which can only be accessed by staff who have been security vetted.</p> <p>Physical and remote access to it is limited by security policies and measures such as only using secure/encrypted communication protocols such as SSH and HTTPS. Also we only grant access to data to users who need that access (i.e. user/group-level authentication and authorisation).</p>
<p>Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?</p>		<p>Yes – as outlined in 5.3 above, our backups are transferred between our UK data centres using an encrypted connection.</p>

Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?		N/A
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, we have an automated schedule for data destruction of various types as defined within our Privacy and Data Policy, under the section entitled ‘How long does EducationCity keep data?’ The data destruction schedule is reviewed every 2 years or when a change occurs to our business processes : <a href="http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy">http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy</a>
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, in accordance with the answer provided in Q5.10 above, all personal information is destroyed once the account is inactive and the data no longer required. Devices on which personal information has been used thoroughly wiped prior to disposal in a safe and certificated way.
Q 5.12 – Does your service provide a mechanism free of charge whereby users can access a complete and secure copy of their data?		This is available within the cloud service and is downloadable directly by the school, free of charge.

## 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 EducationCity is likely to comply with the DPA in relation to data integrity EducationCity Ltd 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?		We use the services of David H Taylor, Data Protection Consultancy Limited, 29 Shadwell Lane, Leeds, LS17 6DP to conduct our independent data audits.
Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers?		Our audits are not published as they are business confidential. However, we act on findings and implement a best practice approach.
Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards?		We aim to follow best practice at all times and follow the expert guidance provided by Data Protection Consultancy Limited whose own security systems are ISO27001 compliant.

Q 6.4 – Are audit trails in place enabling users to monitor who is accessing their data?		All access to our cloud service is via logins at school level. There is an audit trail within the company that tracks employee logins on our Sales Management System (SMS).
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 – we conduct nightly backups of all customer data onto encrypted media which is stored securely off-site.
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?		We have disaster recovery processes in place but the details of these are business confidential.

## 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 EducationCity Ltd 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?		Yes – we use a high-capacity data centre in the UK and reputable cloud services to provide capacity. All aspects of service provision are continually monitored and are architected to scale horizontally when load requires it.
Q 7.2 – Does your service offer guaranteed service levels?		EducationCity undertakes to “use its reasonable skill in making the service available to you and in ensuring its continuing availability during your subscription.” Full details of the company’s warranties can be found at: <a href="http://www.educationcity.com/uk/terms-conditions-schools">http://www.educationcity.com/uk/terms-conditions-schools</a> . Furthermore we have been providing this service for over 15 years. Our uptime in the 12 months to 21/11/17 was 99.99% excluding most scheduled maintenance.
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?		Full details of the company’s limitation of liability can be found at: <a href="http://www.educationcity.com/uk/terms-conditions-schools">http://www.educationcity.com/uk/terms-conditions-schools</a> .

## 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”*

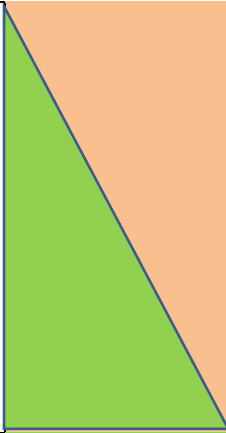
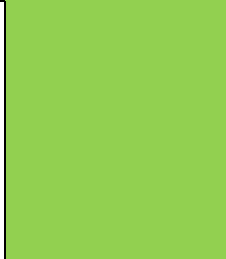
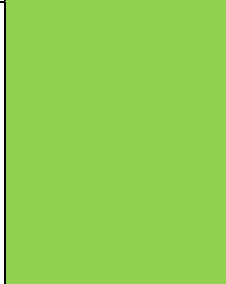
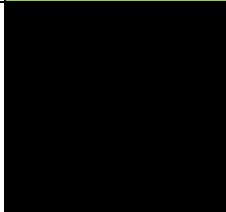
Guidance on data transfers published by the ICO states:

*“Cloud customers should ask a potential cloud provider for a list of countries where data is likely to be processed and for information relating to the safeguards in place there. The cloud provider should be able to explain when data will be transferred to these locations.”*

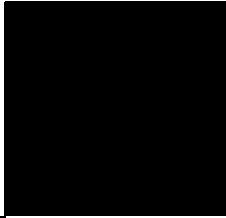
The European Commission has approved four sets of standard contractual clauses (known as model clauses) as providing an adequate level of protection where data is transferred outside the EEA. If your service provider uses these model clauses in their entirety in their contract, you will not have to make your own assessment of adequacy.

To assist schools in understanding where its data is likely to be held and if the cloud service being provided is likely to comply with the DPA in relation to permitted transfers of personal data beyond the EEA, EducationCity Ltd has responded as follows:

<b>Question</b>	<b>Supplier Response Code</b>	<b>Response Statement with Supporting Evidence (where applicable)</b>
-----------------	-------------------------------	---

<p>Q 8.1 – In providing the service do you limit the transfer of personal data to countries within the EEA?</p>		<p>Within the cloud service provided there is no transfer of data outside of the EEA. Our data centre is in the UK and none of this data leaves the UK. We do however sometimes receive requests from schools to process data via email and for email we use Microsoft Office 365 whose servers are based in the USA.</p> <p>Schools are encouraged to upload their pupil data directly to our cloud service rather than to email pupil data to us to keep the data solely in the UK.</p>
<p>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?</p>		<p>Yes – for confirmation please see the section entitled ‘Transfer of Data Outside of the European Economic Area’ in our Privacy and Data Policy for Schools: <a href="http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy">http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy</a></p>
<p>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?</p>		<p>As stated in 8.1 above, there are no data transfers outside of the EEA unless a school emails us such data. We have standard contract clauses in place with our parent company and with all US data processors.</p>
<p>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</p>		<p>N/A</p>

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?



## 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.*

<b>Question</b>	<b>Supplier Response Code</b>	<b>Response Statement with Supporting Evidence (where applicable)</b>
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 pupil or staff users via your school cloud service?		Yes – no advertising is ever delivered to customers or users via our 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?

Yes - our undertaking is clearly set out within our Privacy and Data Policy, under the section entitled 'Sharing Data': <http://www.educationcity.com/uk/primary-schools/educationcity-schools-privacy-data-policy>

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

## Table of Contents

Section 1.0.....	Introduction
Section 2.0 .....	Managing Worst Case Scenarios
Section 3.0.....	Key Support Areas
Section 3.1.....	Addressing Serious Incidents
Section 3.2.....	Supplier Responsibilities
Section 3.3.....	Solution Configuration
Section 3.4.....	Restoring Data
Section 3.5.....	Managing Media Attention
Section 3.6.....	Engaging with Child Support Agencies
Section 3.7.....	Engaging with the Wider School Community

## 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](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 which 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](mailto: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.

*Supplier response:*

If you believe there has been any breach of security such as the disclosure, theft or unauthorised use of your ID, you must notify EducationCity immediately by emailing [support@educationcity.com](mailto:support@educationcity.com) or contacting us during office hours on 01572 725 080. Ask for your account manager and they will escalate the issue to the relevant internal party.

We have an Information Security Incident Response Procedure for all serious issues logged, with incidents being reviewed in operational meetings.

Outside of core office hours the company offers an emergency on-call mobile number where a secure message may be left, to be used only in the case of a major data-breach where the issue cannot be more usefully dealt with during core office hours: 07500 117 791.

### **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.

*Supplier response:*

EducationCity has operation, security, disaster recovery and business continuity plans to minimise the probability of, and the impact of any adverse effect on its service as the result of a serious incident.

Where a customer is impacted by a service incident, the company will depending on the nature of the incident, either;

- a) make information available to the customer to assist in resolution of any service impact, or;
- b) offer to shut down access via a particular user account or for an entire school until the issue is resolved, to limit risks, and;
- c) work directly with the individual customer to manage the result of any service impact.

### 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

*Supplier response:*

Once a customer has transferred relevant information to EducationCity via an encrypted file transfer process, the initial configuration of the service is completed on the customer's behalf. Access to the service is then via an HTTPS (SSL) encrypted connection via a web browser or dedicated mobile application.

Our policy is configure access devices to restrict access to information to known locations/computers (IP addresses) and users (SSH keys or user accounts) and to limit access to only those needing access to that information.

### 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.

*Supplier response:*

EducationCity's backup procedure allows for storage for typically up to 9 days and includes a full back up at the end of every working day. Therefore if an incident occurs overnight, customer data can be restored to the state it was 24-hours earlier, on the following **working** day.

Details of the retention policy can be found within our Privacy and Data Policy, in the section entitled 'How long does EducationCity Keep Data?'

A data restore in line with the service data retention policy, can be requested by the customer raising a call via their account manager.

### 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.

*Supplier response:*

In the event of a serious event resulting in significant media attention falling on the school, EducationCity can provide a statement(s) to provide information relating to the service and the associated serious event.

In addition, as required, the company can provide a media ready description of products or technology used to form part of the service to help customers easily describe the incidents to their users and the media.

### 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.

*Supplier response:*

In the event of a serious event resulting in issues relating to child protection, EducationCity can provide support, where appropriate, to assist customers in their engagement with these agencies.

In addition, as required, the company can provide a media ready description of products or technology used to form part of the service to help customers easily describe the incidents to their users and the media.

### 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.

*Supplier response:*

In the event of a serious event resulting in issues relating to the wider school community, EducationCity can provide a statement(s) to provide information relating to the service and the associated serious event.

In addition, as required, the company can provide a media ready description of products or technology used to form part of the service to help customers easily describe the incidents to their users and the media.