

Request for information on the document re: cloud and secure storage posted on the DfE website, response provided by DfE and Schools Commercial team:

The focus of the project is on data security/safety and the need for schools to ask the right data protection questions of suppliers when considering cloud services. Development of the checklist was achieved via Janet, the ICO, internally via PIRAS and DSU and externally via Microsoft/Google/Amazon/Apple. We have publicised initially via NASBM/ASCL/Academy Show etc... to get the message out to schools. We are quite happy to involve all suitable suppliers if they complete the checklist correctly. It is then up to individual schools to make their choice.

Cloud computing offers one way for schools to make savings within their technology budget, and a range of suppliers now offer cost-effective, cloud-based solutions for storage, document management, office productivity applications, and communications.

Although the various opportunities enabled by cloud services are undoubted, there have been many instances reported in the press where sensitive data has not been adequately protected. This is especially important where children's personal data is concerned and has been the main driving force behind this guidance.

The Department has worked closely in conjunction with the Information Commissioner's Office and major educational cloud providers to develop this invaluable resource. Alongside the written commitments from suppliers, schools will now be able to use the guidance to make informed decisions regarding their sensitive data and how they can safely comply with their responsibilities under the Data Protection Act.

Suppliers are invited to complete the attached checklist document together with service commitments for the benefit of schools.

Please submit and queries and return the completed checklist document to schools.ictsupport@education.gsi.gov.uk

Cloud Software Services for Schools

Supplier self-certification statements with service and support commitments

Supplier name	Education Software Solutions Ltd – Reading Cloud. Part of the Parent Pay Group.
Address	11 Kingsley Lodge 13 New Cavendish Street London W1G 9UG
Contact	Parent Pay DPO
Contact email	ess-dpo@parentpay.com
Contact telephone	0333 0150 212

Contents

Cloud Software Services for Schools	1
Supplier self-certification statements with service and support commitments	1
Introduction	3
1. Supplier commitments	3
2. Using the Supplier Responses	4
3. Supplier Response - Overarching Legal Requirements	7
4. Supplier Response - Data Processing Obligations	8
5. Supplier Response - Data Confidentiality	10
6. Supplier Response - Data Integrity	15
7. Supplier Response - Service Availability	16
8. Supplier Response - Transfers beyond the European Economic Area (EEA)	18
9. Supplier Response - Use of Advertising	20
3.1 ADDRESSING SERIOUS INCIDENTS	26
3.2 SUPPLIER RESPONSIBILITIES	27
3.3 SOLUTION CONFIGURATION	27
3.4 RESTORING DATA	28
3.5 MANAGING MEDIA ATTENTION	28
3.6 ENGAGING WITH CHILD SUPPORT AGENCIES	29
3.7 ENGAGING WITH THE WIDER SCHOOL COMMUNITY	29

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 Junior Librarian.net, Eclipse.net and Reading Cloud services, 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 Ajmal Khan 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,
- 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 . <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 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, Education Software Solutions Ltd confirms the position to be as follows for its cloud service, fuller details of which can be found at <https://www.ess-readingcloud.co.uk>

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	Our contract allows a UK school to fully comply with the requirements as a data controller under the UK Data Protection Act.
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	
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	Customer’s contracts are governed by English law and subject to the jurisdiction of the English courts.
Q 3.4 – Do your services ensure that schools are able to comply with their	YES	Users have access to their own information from within the services.

obligations with regard to the exercise of data subjects' rights?



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 Education Software Solutions Ltd is likely to comply with the DPA in relation to data processing, Education Software Solutions Ltd 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	Education Software Solutions Ltd are the data processor. Each school remains the data controller.
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	Education Software Solutions Ltd 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	Education Software Solutions Ltd adheres to the Group Information Security policies and accompanying standards, of which an overview is available on request.
Q 4.4 – Is the processing of personal data or metadata limited to that necessary to deliver [or improve] the service?	YES	Education Software Solutions Ltd only process data in accordance with the customer agreement and will not process this data for any other purpose.

This document is only valid on the day of printing

Information and Guidance on Cloud Services

Classification: Commercial in Confidence

Version: 1.0

Author: Security Software Test Analyst

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?

YES

Education Software Solutions Ltd has a Data Sharing and Processing document available which should satisfy most customers.

Should the customer also require a separate data processing agreement, Education Software Solutions Ltd has a standard Data Processing Agreement template available for these requests.

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 Education Software Solutions Ltd is likely to comply with UK law in relation to data confidentiality Education Software Solutions 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	Personal data and metadata is retained only for the service provided, and the associated Service Desk and Escalation teams required fault investigation/resolution. Any other use of the personal data or metadata is subject to customer requirements (e.g. other services purchased).
Q 5.2 – Do you prohibit personal data or metadata being shared with third parties?	YES	Personal data and metadata is retained only for the service provided, and the associated Service Desk and Escalation teams required fault investigation/resolution.
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 details are encrypted by using 256Bit SSL (HTTPS) connections. User access to the management area is based on individual usernames and passwords. A defined password policy can be enforced by the data controller to ensure the use of complex passwords.
Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?	YES	Education Software Solutions Ltd internal policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process personal data.
	YES	Education Software Solutions Ltd has controls in place with respect to accessing customer data both within the

Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?



cloud service environment and when extracted for fault investigation/resolution. Access to customer data for fault investigation/resolution is via an Access Control List.

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.

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

All users are forced to use SSL encrypted communications.

Q 5.7 – Does your cloud service ensure that data at rest is encrypted?	YES	Encryption of personal data at rest is a feature which can be enabled within the application. A list of the fields which are encrypted is available on request.
Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?	YES	All data transferred between data centre is encrypted in transit.
Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?	YES	Services provided by Education Software Solutions Ltd can support encryption between other cloud service providers.
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	Data Destruction and deletion is defined in the Education Software Solutions Ltd Customer Data Usage, Transit and Retention Policy. A customer accessible summary of this is available.
Q 5.11 – Does your service ensure that you use a secure deletion and erasure process	YES	Education Software Solutions Ltd has a secure deletion and erasure process which encompasses all copies of the

<p>which encompasses all copies of client/customer data?</p>		<p>customer's data. Where appropriate, an approved destruction and recycling organisation is used.</p>
<p>Q 5.12 – Does your service provide a mechanism free of charge whereby users can access a complete and secure copy of their data?</p>	<p>YES</p>	<p>A complete and secure copy of the customer's data is available on request, subject to authorisation by a senior customer representative in a common format e.g. csv file.</p>

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 Education Software Solutions Ltd is likely to comply with the DPA in relation to data integrity Education Software Solutions 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?	YES	Education Software Solutions Ltd perform regular independent testing by third parties. The platforms which hosts the service is also regularly tested, the relevant documentation can be found at; http://azure.microsoft.com/en-gb/support/trust-center/compliance/
Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers?	YES	A summary version of the audits findings are available on request.
Q 6.3 – Does your service ensure that where such audits are carried out, they	YES	All testing is carried out by independent security specialists. They operate to a thorough testing methodology consisting of elements from OSSTMM and OWASP (amongst other standards) which has been approved by both CREST and CESG.

are conducted to best industry standards?		https://www.owasp.org/index.php/The_OWASP_Testing_Framework
Q 6.4 – Are audit trails in place enabling users to monitor who is accessing their data?	YES	Audit trails are available to administrators.
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	Education Software Solutions Ltd solutions are designed to provide full backup and restores in the event of a 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	Education Software Solutions Ltd have a full disaster recovery plan. Certain processes are available on request, the full details of this plan are 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.

This document is only valid on the day of printing

Information and Guidance on Cloud Services

Classification: Commercial in Confidence

Version: 1.0

Author: Security Software Test Analyst

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 Education Software Solutions 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	Education Software Solutions Ltd continually monitors its cloud services to ensure that there is sufficient capacity available to meet the demand from customers. In addition, where possible, all services have multiple layers of redundancy and resilience built in to minimise, and where possible remove, the impact of any single point of failure.
Q 7.2 – Does your service offer guaranteed service levels?	YES	Subject to contractual agreement, guaranteed service levels can be included as part of the service
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?	YES	Subject to contractual agreement, remedies to customers linked to service levels can be included as part of the service

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, Education Software Solutions Ltd has responded as follows:

This document is only valid on the day of printing

Information and Guidance on Cloud Services

Classification: Commercial in Confidence

Version: 1.0

Author: Security Software Test Analyst

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?	YES	Data for customers is stored and processed from within the EEA. See answer to question 8.2 for details of how any data transfers outside the EEA are managed.
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	If a customer is based in a country outside the EEA and would benefit from having their data transferred to a data centre which is also in a country outside the EEA, Education Software Solutions Ltd will always request permission from the data controller prior to the transfer of data to a country outside the EEA.
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?	N/A	
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	YES	Education Software Solutions Ltd ensures that all data stored or processed outside the EEA is in a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This document is only valid on the day of printing

Information and Guidance on Cloud Services

Classification: Commercial in Confidence

Version: 1.0

Author: Security Software Test Analyst

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.

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 pupil or staff users via your school cloud service?	YES	Education Software Solutions Ltd will not serve advertisements to any pupil or staff users as part of the 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	Education Software Solutions Ltd will not conduct any advertisement-related data mining in respect of pupil or staff data or metadata as part of the cloud service

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

Education Software Solutions Ltd will not use for any commercial purpose (or pass on to others) personal data or metadata in respect of pupil or staff users as part of the cloud service

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
- 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 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:

Customers may log any serious issues regarding the use of the service via their usual support provider for the cloud service, or with Education Software Solutions Ltd directly.

Education Software Solutions Ltd has an Information Security Incident Response Procedure for all serious issues logged, with incidents being reviewed in Operational Board meetings.

Further support is available for customer's ServiceNow Portal.

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:

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

Where a customer is impacted by a service incident, Education Software Solutions Ltd 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) 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 Education Software Solutions Ltd 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. Depending on the service, further configuration can then be undertaken via either an application or management portal by the school's administrative user.

Information on the setup of access devices, and on the general usage of the service is available to the customer via their account on ServiceNow.

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:

Education Software Solutions Ltd backup and data retention policy allows for the storage of customer data for typically up to 3 months. A backup of a hosted library system is taken every 5 minutes for that last 35 days to allow more accurate restores to take place. For backups older than 35 days we retain the backup taken at the start of the week up to 3 months. These backups are stored at the data centre.

After 3 months the backups are automatically deleted.

A data restore in line with the service data retention policy, can be requested by the customer raising a case via their usual support partner.

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, Education Software Solutions Ltd can provide a statement(s) to provide information relating to the service and the associated serious event.

In addition, as required, Education Software Solutions Ltd can provide 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, Education Software Solutions Ltd can provide support, where appropriate, to assist customers in their engagement with these agencies.

In addition, as required, Education Software Solutions Ltd can provide 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, Education Software Solutions Ltd can provide a statement(s) to provide information relating to the service and the associated serious event.

In addition, as required, Education Software Solutions Ltd can provide 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.