Cloud Software Services for Schools

Supplier self-certification statements with service and support commitments

Century-Tech Limited

Supplier name	Century-Tech Limited
Address	7A Perrins Lane, London, NW3 1QY
Contact name	Priya Lakhani
Contact email	info@century.tech
Contact telephone	08006126535

Contents

Introduction

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

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

The questions answered in sections 3 to 9 below will give a good indication as to the quality of a cloud 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 Century-Tech Limited 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 Priya Lakhani who is a senior company official. Priya Lakhani may be contacted on 0800 6126535
- 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. (*It should be made clear that a single "Amber" response is not necessarily a negative, and that any associated clarification should also be considered).*	
Where a supplier is able to confirm that a specific checklist question **does not apply** to their particular service the appropriate self-certification code for that question is **BLACK**.	

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

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

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

3. Supplier Response - Overarching Legal Requirements

Schools are required to ensure that all cloud services used enable them to meet their legal obligations under the DPA. To assist schools in that assessment, Century-Tech Ltd confirms the position to be as follows for its Data Backup and Disaster Recovery service.

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, Century-Tech Limited is registered with ICO as a Data Controller. Consistent with the DPA, Century-Tech Limited offers a written contract that requires Century-Tech Limited shall: *agree that data collected or generated by the Century-Tech Limited relating to user activity to the extent that the data is linked to a user who is a teacher or student of the Customer, is Personal Data and the Customer and the Century-Tech Limited Provider are data controllers in common for this Personal Data; will process Personal Data only in accordance with instructions from the Customer; have in place appropriate technical and organisational measures to safeguard the Personal Data from any unauthorised and unlawful processing,*

		accidental loss, damage, alteration or disclosure.
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 Compliant as above
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, Century-Tech Limited is a UK company offering only UK-based Data Storage so the contracts are enforceable in the UK.
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?		Yes, as part of our service, schools act as Data Controllers. They have sole access to the schools data and are therefore able to comply with their obligations in relation to subject access requests, correction, deletion and blocking of data subject data. Century Tech Ltd will not respond directly to any such request from a Data Subject or third party but will assist the Customer, at its own cost, with all such requests for information within the timescales required by the Customer to allow the request to be dealt with in accordance with the DPA

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 Century-Tech Limited is likely to comply with the DPA in relation to data processing, Century-Tech 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?		Century-Tech Limited is a registered Data Controller to ensure total compliance with ICO. For cloud services, Century-Tech acts as a data controller for customer account information (eg billing information, administrator information).
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, our contract states that Century-Tech Limited only acts on instruction from the Data Controller and will only process data in accordance with the Data Protection Act.

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, our contracts state the specific security measures in place to protect customer data for each of our services. All our measures meet or exceed the requirements of the Data Protection Act. The customer has the right to audit and Century-Tech Limited will, upon request, prepare a report on the technical and organisational measures it has in place to protect the Personal Data it is Processing on the Customer's behalf.
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 data and metadata is only ever processed for the purpose of delivering the service. Where Century-Tech Limited is required, as defined within the DPA, by an instrument of law to provide Personal Data for the purpose of legal proceedings, Century-Tech Limited will notify the Customer immediately and provide a copy of the instrument.
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 the Century-Tech Ltd contracts cover every aspect 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 Century-Tech Ltd is likely to comply with UK law in relation to data confidentiality Century-Tech 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, Century-Tech Limited only uses data provided by the customer in order to provide the cloud services.
Q 5.2 – Do you prohibit personal data or metadata being shared with third parties?		Century-Tech Limited does not share personal data or metadata with third parties except Where such third parties are involved in the delivery of the Century-Tech service, such as AWS. Any third party will have in place a contract containing terms no less robust than that between Century-Tech Limited and its customer.

		Century-Tech will not use the services of any sub-contractors in connection with the processing without prior notification to the customer. Where the customer may explicitly use the service to do so (for example, sharing attendance and performance data with parents) Where the customer grants Century-Tech specific written permission to do so (for example sharing summary data with their Local Authority)
Q 5.3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts?		Yes, Century-Tech Limited has robust security and authentication processes in place to protect access to personal data and user accounts. Customer data is stored in a separate database with restricted access from essential employees only. Our data centre provider, Amazon Web Services (AWS) provides robust security, isolation and encryption, and meets the requirements of ISO 9001, 27001, 27018 https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf
Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?		Yes, Century-Tech Limited has user account logins and Google login authentication for parent log-in and provides administrative controls and reports to help schools protect access to data and accounts

Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?		Yes, Century-Tech Limited expressly commits that: *access to the Personal Data is restricted to only those employees of the Service Provider that are directly related to the Purpose and have a need to access the Personal Data in the course of their employment.*

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, Century-Tech Limited encrypts data that customers provide us that is transmitted over public networks
Q 5.7 – Does your cloud service ensure that data at rest is encrypted?		Yes. Data is stored securely on our servers and encrypted at rest within our data centres. There are extensive physical and electronic measures to prevent unauthorised access.
Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?		Yes, using standard SSL encryption
Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?		Yes, email traffic from Century-Tech Ltd to other cloud service providers is encrypted by default.
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 typically delete customer's data no later than 180 days after the contract end, or within 21 days of the date on which the customer requests the data be deleted.

Q 5.11 – Does your service ensure that you use a secure deletion and erasure process which encompasses all copies of client/customer data?		Yes
Q 5.12 – Does your service provide a mechanism free of charge whereby users can access a complete and secure copy of their data?		Yes, customers can see aggregated and individual data via tools provided by Century-Tech Limited. In the event that they wish to see a complete and secure copy of their data, they can request this from Century-Tech Limited 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 Century-Tech Ltd Data Protection is likely to comply with the DPA in relation to data integrity Century-Tech Ltd Data Protection 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		Yes, Century-Tech Ltd has annual penetration/vulnerability tests performed by a trusted 3rd

third party to conduct regular detailed security audits of the physical, technical and organisational aspects of your service?		party partner. In addition, an independent third party audits the security of the computers and computing environment used in processing data our customers provide. These audits take place annually by qualified, independent security professionals.
Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers?		Yes, upon request by the customer, a confidential summary of the report will be provided to Century-Tech Limited customers. The report will disclose the scope of the report and material findings by the auditor.
Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards?		Yes, all audits are carried out according to the internationally recognised ISO 27001 standard for Data Protection and Security.
Q 6.4 – Are audit trails in place enabling users to monitor who is accessing their data?		Yes, within the Century-Tech Ltd service, logs are produced whenever an 'event' happens with any client account. These reports are available to Century-Tech Ltd technical staff and customer administrators who can view logs for individual user accounts. The logs are extensive and provide details such as date, time, IP address of the machines accessing the account, length of time of access, changes made to the system etc, using the logging platform Logstash.
Q 6.5 – Does your service ensure you could restore all customer data (without		Yes. Century-Tech Limited has robust backup, restore and failover capabilities to ensure availability, business continuity and rapid recovery. All customer data can be

alteration) from a back-up if you suffered any data loss?		restored without alteration from a back-up in the event of a data loss. Daily backups are kept for 180 days and weekly backups kept for 104 weeks.
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, Century-Tech Ltd has full Disaster Recovery and Business Continuity plans in place which are tested regularly.

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 Century-Tech 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, Century-Tech Ltd has sufficient capacity and via our platform monitoring we are able to view and predict potential and physical server storage. Century-Tech Ltd maintains a substantial buffer zone to allow for data fluctuations and capacity can be increased with minimal notice.
Q 7.2 – Does your service offer guaranteed service levels?		Yes Century-Tech Ltd services offer guaranteed service levels to customers.
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?		The Century-Tech Ltd service has never had a claim against it for failure to meet service levels. However, remedies for unmet service levels can be provided within the service level agreements with customers.

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, Century-Tech Ltd as responded as follows:

Question	**Supplier Response Code**	**Response Statement with Supporting Evidence (where applicable)**
Q 8.1 – In providing the service do you limit the transfer of personal data to countries within the EEA?		Yes, the Century-Tech Ltd Data Centres are exclusively UK and EEA based.
Q 8.2 – If you transfer data outside the EEA do you explain to schools when (and		N/A Century-Tech Ltd does not transmit data outside of the EEA.

under what circumstances) data will be transferred to these locations?	[redacted]	
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 As above
Q 8.4 – If you transfer data outside the EEA, (and do not offer the unmodified EU approved "model clauses", can you confirm that the requirements of the DPA are met in respect of the need for adequate protection for the rights and freedoms of data subjects in connection with the cross-border transfer and processing of their personal data?		N/A As above

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		Yes, Century-Tech Limited has made a commitment that it will not use data provided by customers to deliver advertising or for similar commercial purposes.

advertisements to any pupil or staff users via your school cloud service?		
Q 9.2 – In providing the cloud service, is the default position that you enter into a legally binding obligation not to conduct any advertisement-related data mining in respect of pupil or staff data or metadata?		Yes, Century-Tech Limited has made a commitment that it will not use data or information derived from such data provided by customers to deliver advertising or for similar commercial purposes.
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, Century-Tech Ltd will not use personal customer data provided through the use of our cloud services for any advertising or similar commercial purposes, and will not sell customer data provided to us through the use of our cloud services.

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

Table of Contents

Section 1.0 Introduction

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

- Responsibilities in respect of Data Protection Act compliance. General guidance for schools can be found at http://ico.org.uk/for_organisations/sector_guides/education
- The general levels of security inherent in the solutions offered by many of cloud service providers as compared to what might apply to their current arrangements – this information is provided in the general guidance statements to be found at (hyperlink tba.gov)
- The data protection implications of using a particular supplier's cloud services – addressed through the self-certification process detailed in the associated checklist document found above
- The normal support mechanisms available in respect of routine administrative or technical support issues – this is addressed by inviting cloud service providers who are participating in the self-certification process to complete the statements summarising their routine support arrangements as above.
- **The additional support** that would be available in the unlikely event of some **serious data-related incident** related to the use by schools of cloud services – this is addressed by inviting cloud service suppliers to indicate how they would respond to a number of specific challenges 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: Century-Tech Ltd offers a totally transparent service whereby any customer who feels that he/she is not being dealt with appropriately can speak directly with the senior managers and the CEO to help resolve the issue. When a school has any support issues, serious or minor, they should notify Century-Tech and register a Support Call, stating the nature of the issue. This will allow a Support Request Number to be issued allowing the issue to be monitored,

tracked and audited. To register a support call, please call our CTO Kevin Schmidt on 0800 6126535 or email support@century.tech. Technical support is available 24/7/365 and will be provided free of charge.

If the issue is not technical, but relates to data protection and / or privacy, please state this so that the appropriate support team and process can be initiated.

Please always state the nature and severity of the issue.

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:
The free support, with its processes for management, escalation and audit trails is designed to handle all types of issues, including technical, data protection and privacy.

To ensure proper tracking and escalation, we highly recommend that any support call is logged so that Century-Tech can implement the appropriate formal support mechanisms to ensure the incident or issue is addressed effectively, with tracking and audit trails in place.

When using the escalation process and talking to the CEO or Senior Manager, please ensure that the Service Request Number is quoted, with a summary of the issue or incident and its severity. Century-Tech will then respond and ensure resolution of the issue.

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:

The Century-Tech Ltd service is specifically built for UK Educational establishments and is straightforward to configure and use safely.

Password policies are universal and enforced by the Century-Tech service. Other configuration options are designed to prevent accidental sharing of personal data and sensitive personal data.

All Century-Tech Ltd partners and support staff are fully trained in the configuration and deployment of our services which all provide appropriate security as standard.

Appropriate access control policies and suitably complex passwords should be put in place by the school in line with other system policies. The school will always remain the Data Controller under the Data Protection Act.

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:

The Century-Tech Ltd service is specifically designed to protect against such an occurrence. Schools should contact the support team in the first instance which is available 24/7.

Multiple historical restore points are available for immediate restore at any time of day or night as part of our standard operating procedures. Timescales depend entirely on the amount of data that is to be restored.

Data recovery can be in the form of individual files and folders or entire backup sets. All data is returned in its encrypted format to ensure total data security whilst in transit.

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:

If a school was to experience a serious event involving the Century-Tech Ltd service it is vital that they contact our support team on 0800 6126535 or by emailing support@century.tech immediately and register a Support Call, stating the nature and severity of the issue.

Registering the incident and notifying of the significant media attention – both at national and local level - will allow us to address the problem straight away.

Senior members of Century-Tech Ltd will contact, assess and offer advice to the school on how to manage the media attention. However we will never directly discuss the account with any unauthorised persons or persons from the media without prior approval from the school.

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 first instance the school should contact the Century-Tech Ltd Support team on 0800 6126535 or by emailing support@century.tech immediately and register a Support Call, stating the nature and severity of the issue.

The Century-Tech Limited service is specifically designed to protect against losses such as these within a school environment with multiple historical copies of the data held in separate UK Data Centres.

In the highly unlikely event that a school has lost sensitive data from their primary environment and subsequently that data being unavailable from either of the Century-Tech Ltd Data Centres, senior members of Century-Tech Ltd will contact, assess and, and if necessary, engage with the school in any resolution.

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 highly unlikely scenario of a serious incident whereby the wider school community is effected the school must in the first instance report this to our support team on 0800 6126535 or by emailing support@century.tech immediately and register a Support Call, stating the nature and severity of the issue.

The Support Team will endeavour to provide all possible support in dealing with the incident. Senior Managers from Century-Tech Limited would take the lead in discussing the incident and its implications with the authorised account persons with a view to providing advice on dealing with the relevant organisations.