Cloud Software Services for Schools

Supplier self-certification statements with service and support commitments

Please insert supplier details below

Supplier name	Planet Enterprises Ltd
Address	The Old School, 690 Bradford Road, Birkenshaw, West Yorkshire, BD112DR
Contact name	John Stowe
Contact email	john@planetestream.co.uk
Contact telephone	01274 713425

Contents

Introduction

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

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

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

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

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

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

1. Supplier commitments

In order that schools can be confident regarding the accuracy of the self-certification statements made in respect of the **Planet eStream 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 **John Jackson** 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:

- o the checklist question
- o the checklist self-certification response colour
- o 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, **Planet Enterprises Ltd** confirms the position to be as follows for its **Planet eStream Cloud** service, fuller details of which can be found at **www.planetestream.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 - Planet eStream Cloud contract documentation allows Schools to comply with the requirements of the DPA and GDPR.
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 - Our standard contracts are consistent with the DPA and GDPR.

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 - Planet Enterprises Ltd is a UK registered company, Company number 03080901. Our contracts are governed by English Law.
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 - the Planet eStream Cloud service includes administrative tools to enable Schools to fulfil obligations relating to data subject requests.

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 **Planet eStream** is likely to comply with the DPA in relation to data processing, **Planet eStream** 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?	🟩	Planet Enterprises Ltd is a data processor acting on behalf the School using the Planet eStream Cloud service. The only exception is that Planet Enterprises Ltd is a data controller for customer account related information (e.g. billing and administrative 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 - Planet Enterprises Ltd acts according to the instructions of the data controller as provided in the contractual terms.
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 - Planet eStream Cloud contract documentation includes assurances of best practices in relation to Data Protection, Security and resilience of the services provided.
Q 4.4 – Is the processing of personal data or metadata limited to that necessary to	🟩	Yes - The processing of personal data is limited to that necessary to deliver or improve the Planet eStream

deliver [or improve] the service?	🟩	Cloud services.
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?	⬛	The Planet eStream Cloud contract agreements cover relevant aspects of data processing carried out in the provision of the services.

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 **Planet eStream** is likely to comply with UK law in relation to data confidentiality **Planet eStream** 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 or metadata provided by the customer is used only for purposes consistent with provision of Planet eStream Cloud services and is not shared with any other services we may provide.
Q 5.2 – Do you prohibit personal data or metadata being shared with third parties?	🟩	Yes - Personal data or metadata provided by the customer is not shared with third parties.
Q 5.3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts?	🟩	Yes - robust authentication processes are in place and all data passed is encrypted. Authentication integrates with common Directory Services and methods (e.g. Microsoft AD, Azure, ADFS, Shibboleth, Google)
Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?	🟩	Yes – the Planet eStream Cloud service incorporates the principles of 'Privacy by Design' and 'Privacy by Default' and includes secure and granular access control policies to manage access to media content and metadata.
Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?	🟩	Yes - customer data is only accessible to authorised staff and confidentiality agreements are in place for all Planet eStream staff with such access.

<table>
<tr><td></td><td>🟩</td><td></td></tr>
<tr><td colspan="3"><em>Questions 5.6 to 5.9 address the supplier approach to data encryption. The ICO guidance on encryption is as follows:</em>
<em>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.</em>
<em>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.</em>
<em>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/</em>
<em>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.</em></td></tr>
<tr><td>Q 5.6 – Does your cloud service insist that communications with access devices are encrypted?</td><td>🟩</td><td>Yes - All client communications to the Planet eStream Cloud servers are encrypted using HTTPS (TLS) connections.</td></tr>
</table>

Q 5.7 – Does your cloud service ensure that data at rest is encrypted?	🟧	Yes - Central Planet eStream Cloud services are hosted on the highly secure Microsoft Azure infrastructure. By default, data at rest in Microsoft Azure SQL server databases is encrypted. Planet eStream Connect service databases may contain user names as submitted on service registration which are not encrypted at rest. No other personal data is stored in these eStream Connect Service databases.
Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?	🟩	Yes - core Planet eStream Cloud services are hosted on the highly secure Microsoft Azure infrastructure. All data transfers between Microsoft Azure data centres are encrypted.
Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?	🟩	Planet eStream uses Microsoft Exchange Online for email communications. By default, Exchange Online always uses opportunistic TLS. This means Exchange Online always tries to encrypt connections with the most secure version of TLS available. Email communications with other compatible mail servers will therefore be 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 - contract agreements define data retention policies. Data will be securely deleted after 60 days following end of contract.

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 - Planet eStream Cloud services ensure that all customer data can be securely and permanently deleted as required.
Q 5.12 – Does your service provide a mechanism free of charge whereby users can access a complete and secure copy of their data?	🟩	Customer administrators may download media and metadata at any time during contract. Access will be granted by the Supplier for export of the Customer’s media by the Customer for a period of 60 days following end of contract. Additional charges would only be incurred if the customer exceeded agreed bandwidth quotas.

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 **Planet eStream** is likely to comply with the DPA in relation to data integrity **Planet eStream** 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 - Planet eStream Cloud services are audited periodically by an independent third party to verify the security of its software, operations and processes. Microsoft provides details of its compliance certifications and procedures regarding the Azure platform and services in its Trust Center resources https://www.microsoft.com/en-us/trustcenter
Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers?	🟩	A summary of security audit findings can be made available on request.
Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards?	🟩	Security audits are carried out with reference to ISO 27001
Q 6.4 – Are audit trails in place enabling users to monitor who is accessing their data?	🟩	Yes – tools are included to enable customer Administrators to retrieve detailed statistics and reports of their organisation's usage, including viewing activity for media content and activity by individual users.

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 - Data integrity is robustly protected by the levels of redundancy provided in the Microsoft Azure platform, including local and global replication and backup practices. Additional regular backups are deployed by Planet eStream to minimise any loss of data due to, for example, erroneous deletions made by service users, allowing data to be restored without alteration if necessary.
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 - Planet eStream Cloud services are supported by robust disaster recovery planning. Overview can provided on request.

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 **Planet eStream** 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 – the high availability of Planet eStream Cloud services is strongly supported by the levels of resiliency provided by the Microsoft Azure hosting platform and by service monitoring tools deployed in-house by Planet eStream technical services.
Q 7.2 – Does your service offer guaranteed service levels?	🟩	Yes - a Service Level Agreement is supplied as standard practice within the contractual agreements.
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?	🟧	SLA's are provided as standard practice and Planet eStream endeavours to meet or exceed these commitments. Appropriate remedies may be offered based on individual circumstances, goodwill and contractual agreements, in the unlikely event of significant deficiencies in service fulfilment occurring.

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, **Planet eStream** has responded as follows:

Note: On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield which is designed to replace the previous “Safe Harbour” arrangements. Interim guidance in respect of data transfers outside the EEA has been produced by the ICO.

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?	🟩	Planet eStream Cloud services provisioned for customers based in the UK and EEA countries, are hosted in EEA located data centres. Data relating to these services is not transferred outside the EEA.
Q 8.2 – If you transfer data outside the EEA do you explain to schools when (and under what circumstances) data will be transferred to these locations?	⬛	N/A
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 for the rights and freedoms of data subjects in connection with the cross-border transfer and processing of their personal data?	[redacted]	N/A

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?	🟩	The Planet eStream Cloud service does not deliver advertisements to its users.
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?	🟩	The Planet eStream Cloud service does not process or use any personal data or metadata provided by the customer for advertising or similar commercial purpose.

	🟩	
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?	🟩	Personal data or metadata stored in the Planet eStream Cloud service is not used for any other commercial purposes, including advertising, profiling or passing on to third parties

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.

If a potentially serious issue arises regarding the Planet eStream Cloud service provision, this should be raised with the eStream Support Team. The Support Team is the single point of contact for raising technical or security issues and the incident is then routed as required to achieve resolution.
The Support Team can be contacted by email at support@planetestream.co.uk or by telephone on at +44 (0)1274 713425.
The Support Team is available between the hours of 9am and 5pm Monday to

Friday excluding bank and public holidays and the Christmas period from noon on 24th December until 2nd January or nearest working day.
Each request for support is ticketed on our support ticketing system and is prioritised dependent on the severity of the issue reported. We do however ensure that we respond to all requests for support.
When logging a call, please make it clear if it is a serious incident and also if the incident specifically involves Data Protection or Security issues.
Supplying as much relevant information as possible will enable the team to identify if the incident requires escalation to Senior Technical staff or Senior Management where appropriate.

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.

Our Support Team endeavours at all times to meet or exceed the expectations as detailed in our standard Service Level Agreements.
Planet eStream also aims to be as flexible and accommodating as we can of customer requirements and deadlines and we are extremely diligent in attempting to minimize ‘Down Time’ for our clients. Serious service affecting incidents are given the highest priority in order to achieve resolution as rapidly and effectively as possible.
Any incident that may have implications regarding the safety or security of our users will by default be treated with the highest priority, so that risk can be identified and assessed immediately and appropriate actions taken commensurate with the level of risk.
The Support Team ticketing system enables the progress of incidents to be tracked and audited to ensure efficient resolutions are achieved.

The Support Team office operates during hours as indicated in section 3.1 above. Monitoring of emails by senior Planet eStream staff is not restricted to these hours however, so reports of serious incidents may receive attention outside of these hours where this is practical and appropriate.

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

When an organisation subscribes to the Planet eStream Cloud service, relevant staff members receive a Technical Handover, typically via a web meeting. The aim of these sessions is to enable the Schools to configure suitable levels of user access privileges for Administrators, general staff and student users as applicable. Customisation of the user interface is also addressed at this point.
Additional end user training sessions may also carried out by arrangement with our Training team.

A selection of technical and user experience resources are available online
https://www.planetestream.co.uk/support.aspx

The Planet eStream Cloud service is designed to be easy to engage with for end user clients. A wide range of devices are supported and access is primarily achieved using standard Web browsers over secure HTTPS connections. Default settings are typically suitable for this purpose.

The Planet eStream Cloud service does support creation of local ‘Built-In’ user access accounts, but in general user authentication is integrated with existing Directory Services in use by the School and password and other security policies will therefore largely be defined by the infrastructure currently in place. We would suggest that if ‘Built-In’ users are deployed, similar policies regarding password strength are used in these cases.

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.

Planet eStream Cloud core services are hosted on the highly resilient Microsoft Azure platform. The computing, storage and database asset deployments are designed to achieve very high levels of service continuity, data integrity and security. Data integrity is underpinned by the use of locally and globally replicated data storage. In the unlikely event of data loss due to hosting platform issues, regular database and media content backups are also taken, from which customer data can be restored if required to minimise the impact of such a failure.

Planet eStream does not delete or manage customer data as part of the service provision. The management of customer data is the responsibility of the School, which is the data controller. Deleting media content using the eStream web interface take the media 'offline' and the files are then stored in a 'recycle' area. Media can be restored very quickly from the 'recycle' area by a School eStream administrator using the relevant management tool. Permanent deletion of data, if required, is an active process carried out by a School eStream administrator using this management interface.

Media that has mistakenly been permanently deleted can potentially be restored from our backups. Arrangements can be made by raising a ticket with the Planet eStream Support Team.

Data backup retention time targets are 90 days for media files and 30 days for SQL databases.

The only occasion when Planet eStream will permanently delete customer data is to fulfil the 'end of contract' commitment to fully and securely erase data 60 days after the service provision has ceased.

Data restoration from backups can usually be achieved within a working day, although in some cases where large amounts of data are involved, the restore copy process could take longer to complete.

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.

If a serious event occurs that may relate to use of Planet eStream Cloud services, the School should immediately raise a ticket with the Planet eStream Support Team, as detailed in section 3.1 above. When logging a call, please make it clear if it is a serious incident and also if the incident specifically involves media attention and provide as much detail as possible about the nature of the event and if local or national media are involved.

Senior members of the Planet eStream staff will work with the School to assess the incident and, if necessary, engage directly to assist in managing the media attention to a resolution.

In such cases it would also be advisable to engage with your Local authority, relevant governing body or trustees for guidance and advice.

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.

If a serious event occurs that may relate to use of Planet eStream Cloud services, the School should immediately raise a ticket with the Planet eStream Support Team, as detailed in section 3.1 above. When logging a call, please make it clear if it is a serious incident and also if the incident specifically involves child protection and support agencies and provide as much detail as possible about the nature of the event.

Senior members of the Planet eStream staff will work with the School to assess the incident and, if necessary, engage directly to assist in managing the child protection incident to a resolution.

In this case it would also be advisable to engage with your Local authority, relevant governing body or trustees for guidance and advice.

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.

If a serious event occurs that may relate to use of Planet eStream Cloud services, the School should immediately raise a ticket with the Planet eStream Support Team, as detailed in section 3.1 above. When logging a call, please make it clear if it is a serious incident and provide as much detail as possible about the nature of the event and indicate bodies and organisations from the wider school and education community that may be involved.

Directors of Planet eStream have broad experience of liaising with a wide range of educational, commercial and public sector bodies and organisations and can reach out to the School to assess the incident and, if necessary, engage directly to assist in managing the incident to a resolution.