SQUAD
IN TOUCH

Cloud Software Services for Schools

Supplier self-certification statements with service and support commitments

Please insert supplier details below

Supplier name	Squad In Touch LTD
Address	Basepoint Business Centre, Metcalf Way | Crawley, RH11 7XX
Contact name	Vadim Shchepinov
Contact email	v.shchepinov@squadintouch.com
Contact telephone	07909120045

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 Squad In Touch 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 Olesya Rodicheva 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. (*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, Squad In Touch LTD confirms the position to be as follows for its Squad In Touch service, fuller details of which can be found at www.squadintouch.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 standard contract for the supply of Squad In Touch as a cloud service allows schools 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 - see the answer to Q 3.1

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** – Squad In Touch LTD is a company registered in England and Wales, company number 9657481, and our contract is 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** – Squad In Touch cloud service supports role- and object- user permission model thus ensuring schools are able to fully comply with their 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 Squad In Touch LTD is likely to comply with the DPA in relation to data processing, Squad In Touch 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?	🟩	Squad In Touch LTD does not act as a data controller with regards to their cloud service. The schools are the Data Controllers and Squad In Touch LTD acts as a Data Processor on behalf of the schools. (see paragraphs 12.3, 12.4 of our Terms and Conditions for schools).
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 Squad In Touch LTD only acts as a Data Processor and will only process data in accordance with the Data Protection Act (see paragraph 12.5.1 of our terms and conditions).
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 contract states that Squad In Touch LTD implements sufficient technical and organisational steps against unauthorised or unlawful Processing of Personal Data (see paragraph 12.5.4 of our terms and conditions).
Q 4.4 – Is the processing of personal data or metadata limited to that necessary to	🟩	**Yes** – only the users with school admin roles can grant permission to school’s personal data, this includes

deliver [or improve] the service?	🟩	granting permission for Squad In Touch LTD support team members, for the purpose of service delivering or improvement. After such processing of personal data all permissions shall be revoked.
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?	🟩	Although our terms and conditions do cover every aspect of data processing, we are prepared to enter into a separate data-processing agreement to cover any specific customer's needs.

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 Squad In Touch LTD is likely to comply with UK law in relation to data confidentiality Squad In Touch 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 stored and processed by Squad In Touch cloud service is not shared across any other service that Squad In Touch LTD provides. Server instances and databases are separated for each service and each country they are dedicated for. Each server instance and each database are equipped with separate access controls.
Q 5.2 – Do you prohibit personal data or metadata being shared with third parties?	🟩	**Yes** – We do not share personal data or metadata with third parties except where the school uses the service to do so (e.g. school uses the service to publish some information on its dedicated public sport web site, school uses the service to share some information with other schools, parents, their Local Authority, etc.)
Q 5.3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts?	🟩	**Yes** – Squad In Touch cloud service supports role- and object- user permission model which allows users access to only the personal data they are granted permissions for. Squad In Touch cloud service supports user authentication by username and password. Using long enough passwords which contain at least one

	🟩	capital letter and at least one digit is a must for all Squad In Touch cloud service users.
Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?	🟩	**Yes** – only the users with school admin roles can grant permission to school’s personal data. Squad In Touch cloud service assists schools to prove the user identity by verifying their email and telephone number during the sign up process. The users with school admin roles can revoke, partially or entirely, access rights for any Squad In Touch cloud service user at any time.
Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?	🟩	**Yes** – Squad In Touch LTD commits that only Squad In Touch Ltd support team members can have access to customer data when it is necessary for the purposes of service delivering or improvement. Only the users with school admin roles can grant permission to school’s personal data even for Squad In Touch LTD support team members. When users with school admin roles grant temporary permissions to the school data they shall make sure that they provide such access to authorized personnel of Squad In Touch LTD support team to perform certain actions with school's data. After such processing of personal data all permissions shall be revoked.

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 Squad In Touch cloud service users are forced to use SSL (HTTPS) encrypted connection. All communications between server and any type of access devices are fully encrypted. All API communications between servers are also encrypted.

Q 5.7 – Does your cloud service ensure that data at rest is encrypted?	🟩	**Yes** – Squad In Touch cloud service data is securely stored on servers on the cloud. There are numerous measures both hardware and software including encryption which are applied to data at rest to prevent unauthorised access. The most sensitive data (users' passwords) are stored irreversibly encrypted.
Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?	🟩	**Yes** – All API communications between Squad In Touch cloud service servers are encrypted, include communications between servers in different data centres.
Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?	⬛	**N/A** - Squad In Touch cloud service does not communicate with other cloud services via email.
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** - If requested by the customer Squad In Touch LTD will delete any of their data in 3 working days (see paragraph 13.4.4 of our terms and conditions). Squad In Touch LTD obviously needs subscription termination before data deletion because Squad In

	🟩	Touch LTD will not be able to fulfil their obligations under the contract after data deletion. The customer can terminate their subscription at any time free of charge without any obligations (see paragraph 13.1 of our terms and conditions).
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** - If requested by the customer Squad In Touch LTD will delete any their data, including all archive copies (see paragraph 13.4.4 of our terms and conditions).
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** - If requested by the customer Squad In Touch LTD will provide them with a copy of any data which relates to that customer. There is no charge for providing customer's data and the data will be provided as soon as reasonably practicable (see paragraph 12.6. of our terms and conditions).

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 Squad In Touch LTD is likely to comply with the DPA in relation to data integrity Squad In Touch 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** – Squad In Touch cloud service is deployed on Amazon Web Service cloud and we use Amazon Inspector service (see aws.amazon.com/inspector/) monthly. Amazon perform the following tests of Squad In Touch cloud service: - Vulnerability assessment - Incident management processes - Personnel security checks - User access control through support channels - Etc. Amazon is trusted ISO 27001 and UK Cyber Essentials Plus certified services provider.
Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective	🟩	**Yes** - If requested by the customer Squad In Touch LTD will provide the most recent report containing detailed results of the inspection. For prospective

cloud customers?	🟩	customers the report is available in case NDA is signed
Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards?	🟩	**Yes** – our audit service provider is ISO 27001 and UK Cyber Essentials Plus certified.
Q 6.4 – Are audit trails in place enabling users to monitor who is accessing their data?	🟩	**Yes** – Squad In Touch cloud service logs all users data requests. Log file includes user's ID. If requested by the customer, Squad In Touch LTD will provide them with the customer's data access log files.
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** – backups are taken in accordance with Squad In Touch LTD backup policy and are securely stored. Squad In Touch LTD restores data from archive files in the event of system failure or upon the customer's request (see paragraphs 12.7. – 12.9. of our terms and conditions).
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** - Squad In Touch LTD has a full disaster recovery plan. Particular states are available on customers reasoned request. The full details of the disaster recovery plan are for internal use only.

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 Squad In Touch 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** - Squad In Touch LTD hosting platform is elastic and can scale up as required to match the loading. Our technical support team monitors infrastructure constantly and increases its capacity in advance to prevent service slowdown and failure.

Q 7.2 – Does your service offer guaranteed service levels?	🟩	**Yes** - Squad In Touch LTD offers generic guaranteed service level (see paragraphs 7.1., 7.2. of our terms and conditions). Additional guaranteed service levels can be included as part of the service on the customer request.
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?	🟩	**Yes** - Squad In Touch LTD provides a full money back guarantee if the customer is not satisfied with our services, including in the event that service levels are not met. Any requests for cancellation pursuant to the Money Back Guarantee must be received within 30 days of the subscription activation (see paragraph 13.5 of our terms and conditions).

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, Squad In Touch LTD 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	🟩	**Yes** – Squad In Touch cloud service data of the UK schools is stored and hosted on AWS data centres within EEA.

within 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, Squad In Touch LTD does not transmit UK data outside of 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, 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 advertisements to any pupil or staff users via your school cloud service?	🟩	**Yes** – Squad In Touch cloud service does not serve any advertisements to any of their 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?	🟩	**Yes** – data stored on Squad In Touch cloud services is not used for any advertisement-related data mining.
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** – data stored on Squad In Touch cloud services is not used for any commercial purposes.

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:

Customers can input any issues regarding the use of the service via their usual support email, Skype or online assistance system for the cloud service.
If required, serious issues can be escalated directly to the Head of Support Team, Laura Bennett, by email l.bennett@squadintouch.co.uk or by telephone 01293-733139.

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:

In the event of a serious incident the school will have the full 24X7 support of our support team as a priority matter until resolution.

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 initial configuration of the service is completed by Squad In Touch LTD on the customer’s behalf. We also provide any further information and configuration requirements as part of the service offering when the school is signed up.

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:

As stated above, backups are taken in accordance with Squad In Touch LTD backup policy and are securely stored. Squad In Touch LTD restores data from archive files in the serious event which resulted in the loss of data by a school in 24 hours.
A data restore can be requested by the customer calling Squad In Touch LTD support team.

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:

Squad In Touch LTD can provide the school with the clear explanation of that serious event, in language appropriate to the public.
Squad In Touch LTD can provide that explanation to the school to share with whoever they think appropriate.
Squad In Touch LTD can also usually make the explanation public on its site.

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:

Squad In Touch LTD can provide support in whatever way it can to assist customers in their engagement with these agencies.

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:

Squad In Touch LTD can provide statement which contains information relating to the service and the associated serious event.