Cloud Software Services for Schools

Supplier self-certification statements with service and support commitments

Please insert supplier details below

Supplier name	Groupcall Limited
Address	Commerce House, 1 Raven Road, London E18 1HB
Contact name	Steve Baines
Contact email	sbaines@groupcall.com
Contact telephone	020 8506 6190

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 Groupcall 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 Steve Baines, Data protection Officer, 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, Groupcall Limited confirms the position to be as follows for its cloud based services, fuller details of which can be found at www.groupcall.com

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. Groupcall and all of our services fully comply with the DPA and this is confirmed within our standard contract. Our Data Sharing Agreements specify that we will be acting as Data Processors under the direction of the school as Data Controller. We specify that we will not use the data for any other purposes, have implemented appropriate measures to protect the data against improper access, disclosure or loss and that we will comply with the DPA and all applicable laws.
Q 3.2 – If your standard contract does not fully comply with the DPA, do you offer	⬛	N/A – however, in addition to being registered under the DPA we are also accredited to ISO 27001, the international standard for Information Security Management and as such are audited by external

additional commitments to UK schools to help ensure such compliance?	⬛	verifiers each year to ensure we are protecting all data accordingly. We are also authorised suppliers under the UK Government G Cloud Framework with the added reassurance that Groupcall have been approved by the UK Government as meeting all required standards including those for data protection and security.
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 – Groupcall are a UK registered company and our contracts are fully enforceable under UK 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. Groupcall fully comply with all elements of the DPA including data subjects’ rights and can provide reports for schools as required to assist them in addressing and data subject requests to amend, correct, delete or erase their data

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 Groupcall Limited is likely to comply with the DPA in relation to data processing, Groupcall Limited 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?	🟩	Not in relation to the school data – Groupcall act as the Data Processors, with the schools acting as Data Controllers. The exception to this is that we do act as Data Controllers in respect of our own customer account information, such as the school name and address, billing information etc.
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 – this is included in our terms and is part of our data sharing agreement. The school data is owned by the school and not by Groupcall and we undertake not to use this data for any purposes other than that specified in order to provide the services purchased by the school
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 agreements and data protection policies provide this. In addition, our accreditation to ISO 27001 is dependent upon our complying with all aspects of the DPA and we are externally audited annually to ensure compliance with all appropriate data security obligations.

	🟩	
Q 4.4 – Is the processing of personal data or metadata limited to that necessary to deliver [or improve] the service?	🟩	Yes absolutely. The ways we use personal data are detailed in our documentation around security of data and are limited to processing that is necessary for the delivery or improvement of the service and nothing further.
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 – our contracts cover all aspects of the data processing as outlined above

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 Groupcall Limited is likely to comply with UK law in relation to data confidentiality Groupcall Limited 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. We only use data supplied to us by schools for the explicit purpose of delivering the service purchased and do not allow the data to be shared across other services unless also purchased by the school.
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 any third parties unless the school purchases a module from us which is supplied by a partner company. In those circumstances, additional data sharing agreements apply to the data being shared and this can only be shared with the schools express permission and only in order to deliver the services purchased.
Q 5.3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts?	🟩	Yes, it does. Our services have extremely robust authentication processes in place to protect access in any way, including two-factor authentication, unique user names, unique passwords and user lock out after failed attempts to access services.
Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?	🟩	Yes. As well as the multiple authentication measures detailed above, we provide schools with administrative control and reporting to help them protect access to data and/or user accounts

	🟩	
Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?	🟩	Yes. We restrict access to personal data to those staff that require such access in order to perform their roles – these include support staff, trainers etc. who need access to the data to perform the functions required by the schools. Other staff are denied access to the data through the use of permission restrictions, user names and passwords etc. to protect all data from unauthorised access.

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 data in transit is encrypted using industry standard encryption.
Q 5.7 – Does your cloud service ensure that data at rest is encrypted?	🟩	We are compliant with ISO27001 and with DPA regulations. We use Microsoft Azure cloud services for data storage which are located in within the European economic community and those services are also fully compliant with all DPA regulations and have accreditation to a broad set of international and industry-specific compliance standards such as ISO 27001, HIPAA, FedRamp, SOC 1 and SOC 2 as well as country-specific standards including the UK Government G Cloud Framework etc. Encryption is just one of the data security measures that can be applied as part of a multi-layered stack of protective measures for data, the specific choice of encryption approach varies by product and ranges from encryption of high impact data areas such as user credentials and secrets, through full and isolated AES encryption of all data.

Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?	🟩	Yes. All data in transit is encrypted using industry standard encryption, including transfers between Azure datacentres where applicable.
Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?	🟩	Yes. We use opportunistic TLS encryption to encrypt email traffic between our service and recipient email providers.
Q 5.10 – Does your service provide defined timescales in respect of data destruction and deletion both during the contract and at contract end?	🟩	Yes. We delete customer data 6 months after contract end. Customers can also request that we delete data immediately at any time, however this would curtail the service of course.
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. We securely delete all copies of the client/customer data both within their live service and in back up storage too.

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, we are happy to provide a secure copy of customer's data upon request and without 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 Groupcall Limited is likely to comply with the DPA in relation to data integrity Groupcall Limited 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. As part of our ISO 27001 accreditation we are audited annually by external verifiers who conduct detailed security audits of the physical, technical and organisational aspects of our services.

Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers?	🟩	Yes. Customers can request these findings and we can provide a confidential summary of the report from the audit if requested. This summary report will disclose the auditor’s findings across all areas.
Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards?	🟩	Yes. As detailed above, the audits are carried out under the standards imposed by ISO 27001 and the auditors themselves are qualified as Lead Auditors for this standard.
Q 6.4 – Are audit trails in place enabling users to monitor who is accessing their data?	🟩	Yes. Customers can set up users with administrative permissions who can then view the audit logs showing which users have accessed their data with users clearly identified by their unique user names.
Q 6.5 – Does your service ensure you could restore all customer data (without alteration) from a back-up if you suffered any data loss?	🟩	Yes. We have a full back up system in place both onsite and offsite and this enables us to restore all customer data, without alteration, should there be any need to do so. Our cloud storage has full and robust back up, restore and failover capabilities to enable business continuity and rapid recovery in the event of any event.
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. We have a full disaster recovery and business continuity plan which we maintain as part of our ISO 27001 accreditation. These plans are, for obvious reasons, kept confidential but we are able to provide summaries for customers/prospective customers upon 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 Groupcall Limited 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, where our services are cloud-based we operate auto-scaling of server resources to accommodate demand. We partition customers into separate data storage groups to isolate spikes in usage and review the allocation of customers to storage groups on a fortnightly basis.

Q 7.2 – Does your service offer guaranteed service levels?	🟩	Yes. We have Service Level Agreements in place and review these regularly to ensure we both meet these levels and wherever possible can improve upon them.
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?	🟩	Yes. These can be set at a customer or contract level as required.

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, Groupcall Limited 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?	🟩	Yes. As detailed previously, we use the Microsoft Azure cloud in Northern Europe with fail over to Western Europe. We do not transfer personal data outside of the EEA. Were we to require such a transfer (for example, due to a new service offering etc.), we would ensure appropriate safeguards were in place to protect any such data transfers in line with the DPA requirements.
Q 8.2 – If you transfer data outside the EEA do you explain to schools when (and	⬛	N/A

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?	[redacted]	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	🟩	Yes. We have always maintained the position that we will not allow any advertising through our services at all.

legally binding obligation not to serve 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. We have always maintained the position that customer data will not be used for any purpose other than to provide the services requested by the school. Under no circumstances will we allow customer data or meta data to be mined for any advertisement-related 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?	🟩	Yes. This has always and will continue to be our default position. We believe that the personal data or metadata we process is to be used solely for the purposes intended by the customer and will not allow this to be used for any other commercial purpose.

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:

- Should a school have any issues regarding the use of the services, data protection concerns, privacy issues etc., they can log this with our support team by email or telephone (support@groupcall.com or 020 8506 6100). The call should identify the establishment raising the call, the person raising the call including their contact details and a brief description of the problem so that an initial assessment can be made and the case directed to the appropriate technical team

- Once a call is logged with us through email or telephone, the school will immediately receive a response confirming receipt of the call and providing a call log number so that they are able to track their call and so that calls can be monitored and audited
- Support is included within all of our service offerings and will be provided in the best format for the circumstances. This would normally be through email and/or telephone calls but could also include remote screen sharing sessions, authorised access to school systems under the monitoring of the school staff or even onsite support if necessary
- In addition, we provide detailed and in depth online support and guidance including FAQ’s etc. through our support pages at support.groupcall.com
- Cases can be escalated as necessary, both by our own internal teams and by the schools themselves. The first point of escalation is to our Support Team Manager. If necessary, further escalation can be made to our Technical Director.
- Where a school has taken our services through their Local Authority, it is always advisable that they also raise the issues with the authority so that they are also aware of the problem and can liaise with us to resolve issues as swiftly as possible
- Where a serious breach is discovered by Groupcall Limited or communicated to us, we will immediately inform the school concerned and work with them to fully understand the nature and extent of the incident, determine the root cause, design and configure a resolution and restore any data accurately and securely
- Where the situation warrants it, and in agreement with the school concerned, we will liaise with appropriate agencies and the wider school community as necessary

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 above detailed technical support including the escalation process is designed to address and resolve the majority of issues. In cases of a serious incident, we would also work closely with the school to identify the issue and the root cause of this, put into place appropriate resolutions and test to ensure the resolution is robust and successful.

- In serious incidents, the school will have access to its own Account Manager as well as a named support technician or the Support Manager as appropriate.
- Where a school has concerns over data security or Privacy issues, they are able to escalate this immediately to our Data Protection Officer, Steve Baines, via sbaines@groupcall.com or 020 8506 6100.
- We will at all times deal with these issues in a timely and secure manner taking into account the seriousness of the situation and the potential impact on the school, its staff, pupils or parents.
- Where an issue is identified that could or has impacted upon any of these groups, we will liaise with the school to agree the best form of communication with all stakeholders to allay fears, resolve issues and maintain confidence in the school and the service itself.

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:

- Our services are built to be straightforward to configure and deploy and to be used safely and easily by school users. All our services are designed specifically for education users rather than being commercial products adapted for educational use.
- Back up and data synchronisation is taken care of by our services with no requirement for schools to perform any additional tasks.
- We provide additional configuration levels that enable schools to dictate the password policy and strength they require. The administration permissions enable schools to restrict access to the system for their users to a granular level, ensuring that they only allow staff the level of access deemed necessary for their role and use of the service – this could be down to the

level of a member of staff having access to the service for just one pupil in the school if necessary or deemed appropriate.

- Helpdesk and security staff at Groupcall have access restrictions to customer data based around their role and the requirements of the tasks they need to be able to perform for schools and have no access unless they require this to perform their duties.
- All levels of our services, no matter the price point, have the same level of data security as we see this as an essential component of all services we offer.

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 Groupcall Limited cloud services rely on data feeds from the school Management information System (MIS) on a regular (usually overnight) basis.
- In the unlikely event of an incident causing data loss, this data will be automatically restored on the next scheduled synchronisation with the school MIS without need for any manual intervention
- Manual synchronisation can also be performed immediately at any time should this be necessary or where waiting for the next scheduled synchronisation would impact on the service
- A full synchronisation with the school MIS to restore school data into the Groupcall limited services would take a matter of minutes only to perform, restoring all data into the services so that full use of the services can be resumed
- Any data stored in the services, such as incoming text messages etc., are stored by us with back-ups and can be written back into the service in the unlikely event of a data loss

3.5 MANAGING MEDIA ATTENTION

Where a serious event had occurred which resulted in significant media attention falling on the school, suppliers should indicate the steps they would take as a responsible service provider to work with the school in managing the media attention.

Supplier response:

- In the extremely unlikely event of a serious incident impacting on the Groupcall Limited services, the first step should be to raise a support call as soon as possible so that the appropriate resources can be deployed to investigate and resolve the issue
- In the event of a serious incident, the impact or potential impact should be stated along with the person(s) potentially affected and any wider school community that might be affected so that the severity of the incident can be assessed immediately
- Where local or national media attention has been brought, this should be stated to us as soon as possible so that we can work with the school to agree appropriate communications and ensure that the event is handled securely
- Senior members of the Groupcall team will liaise with the school to assess the incident, agree the appropriate response and, where required, engage directly with the media to provide information and resolution measures
- In such a case, we would expect the school to also inform the Local Authority or Academy Chain management of the incident and have them involved in these discussions in advance of engaging with the media wherever possible
- At all times, we believe honesty to be the best policy and would take ownership of any issues that have been caused by our services

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:

- As detailed above, in the extremely unlikely event of a serious incident impacting on the Groupcall Limited services, the first step should be to raise a support call as soon as possible so that the appropriate resources can be deployed to investigate and resolve the issue
- In the event of a serious incident, the impact or potential impact should be stated along with the person(s) potentially affected and any wider school community that might be affected so that the severity of the incident can be assessed immediately
- Where the circumstances warrant the intervention of child protection agencies, Groupcall will work alongside the school and such agencies to assess the impact of the incident, identify those potentially impacted and work to find a resolution to the incident in a timely manner

- We will provide whatever level of assistance is required in these circumstances to protect those impacted and to minimise the potential impact caused by the incident

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:

- As detailed above, in the extremely unlikely event of a serious incident impacting on the Groupcall Limited services, the first step should be to raise a support call as soon as possible so that the appropriate resources can be deployed to investigate and resolve the issue
- In the event of a serious incident, the impact or potential impact should be stated along with the person(s) potentially affected and any wider school community that might be affected so that the severity of the incident can be assessed immediately
- Where the serious incident results in issues raised related to the wider school community we would provide all possible assistance to the school in liaising with the wider community and any agencies involved to investigate, identify and resolve the issue as swiftly as possible and to minimise any potential impact
- Senior members of the Groupcall team will be made available to the school and the wider community to discuss the incident, explain the issues raised and the measures proposed to resolve the incident and minimise impact
- Where it is deemed necessary, this assistance could include telephone liaison, email updates or on-site meetings as appropriate