Cloud Software Services for Schools

Supplier self-certification statements with service and support commitments

Please insert supplier details below

Supplier name	123Comms Limited (Trading as ParentMail)
Address	Litton House, Saville Road, Peterborough, Cambs, PE3 7PR
Contact name	For queries relating to the check list, please contact Alex Joyce, Operations Director
Contact email	Info@parentmail.co.uk
Contact telephone	01733 595959

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 ParentMail 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 Martin Temple 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, ParentMail confirms the position to be as follows for its service, fuller details of which can be found at www.parentmail.co.uk/terms

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 we believe our contract allows a UK school to meet the requirements of DPA. In accordance with the DPA, ParentMail: • only act on customers' instructions • has implemented measures to protect customer data against improper access, disclosure or loss • will comply will all applicable data protection laws
Q 3.2 – If your standard contract does not fully comply with the DPA, do you offer additional commitments to UK schools to help ensure such compliance?		N/A
Q 3.3 – Is your contract with UK customers enforceable both in the UK and in the country in which your company is registered?		Yes, our contract is governed by English Law and 123Comms Limited is registered in the UK (Registration No. 04336436)
Q 3.4 – Do your services ensure that schools are able to		Yes, ParentMail provides tools enabling Schools to correct, delete or block data (parent information). Parents' have the ability to amend or

| comply with their obligations with regard to the exercise of data subjects' rights? | | delete their accounts. |

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 ParentMail is likely to comply with the DPA in relation to data processing, ParentMail 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?		For communication services ParentMail acts as the Data Processor and the customer acts as the Data Controller. We do not use the data for our own purposes or collect any information ourselves. All personal data we hold in connection with our service is provided by the school or parents themselves. For payment services ParentMail acts as a data controller for billing information and user KYC (Know Your Customer Checks).

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, ParentMail only acts upon the instructions of the Data Controller as per the contract.
Q. 4.3 – Does your contract document the security measures that you implement to enable a school to ensure compliance with the DPA's security obligations?		Yes, our contract states that we *'have in place appropriate technical and organisational security measures to protect those data against unauthorised or unlawful processing and accidental loss, destruction or damage.'* The security information is available when requested by our customers.
Q 4.4 – Is the processing of personal data or metadata limited to that necessary to deliver [or improve] the service?		Yes, for clarity ParentMail will only process data in accordance with the contract and will not sell or rent any information to any third party for any reason, outside of the use of our Websites. Please refer to our Privacy Policy at: http://www.parentmail.co.uk/privacy-policy/
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?		Not applicable, ParentMail contract for cloud computing and services covers every area of data processing.

5. Supplier Response - Data Confidentiality

When choosing a cloud service provider, schools must select a data processor providing sufficient guarantees about the technical and organisational security measures governing the processing to be carried out, and must take reasonable steps to ensure compliance with those measures.

The cloud customer should therefore review the guarantees of confidentiality that the cloud provider can commit to. To assist in understanding if the service being provided by ParentMail is likely to comply with UK law in relation to data confidentiality ParentMail 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, ParentMail will only ever process Customer Data in accordance with the instructions received from the Customer and not for any other purpose. Please refer to our Privacy Policy at: http://www.parentmail.co.uk/privacy-policy/
Q 5.2 – Do you prohibit personal data or metadata being shared with third parties?		Yes, for clarity ParentMail will not sell, rent or provide any information to any third party for any reason, outside of the use of our Websites. Please refer to our Privacy Policy at: http://www.parentmail.co.uk/privacy-policy/
Q 5.3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts?		Yes, login is securely encrypted via HTTPS (SSL). ParentMail Admin level access is restricted to specific IP addresses & two factor authentication is employed

Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?		Yes, access to the system is controlled via a secure login and by the granting of permissions. Obtaining access to our service is controlled by a ParentMail Administrator at the school who can grant access and permissions to other authorised School Staff. The 'Permissions function' controls the accessibility to data and to the functionality of the system.
Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?		Yes, as identified above. Our service permits access to data and functionality to be controlled by the ParentMail Administrator when granting permissions to other authorised staff members. Additionally, ParentMail staff access is restricted to those individuals that require such access to perform their role and function.

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.

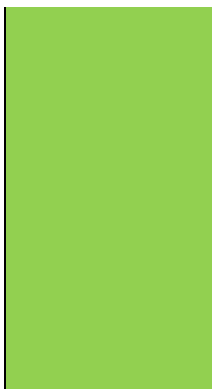|		
Q 5.6 – Does your cloud service insist that communications with access devices are encrypted?		Yes, all data is encrypted.
Q 5.7 – Does your cloud service ensure that data at rest is encrypted?		Yes, all stored data is encrypted and all API communications are also encrypted.
Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?		Yes, all data is encrypted.
Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?		Yes, all data is encrypted.
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, leaving customer data is made inaccessible within 7 days and deleted from the cloud after 90 days. Existing customers can request their data to be deleted immediately (this will terminate their service). The deletion of data will then be fully completed within 30 days to allow for the removal from backup media.

Question	Supplier Response Code	Response Statement with Supporting Evidence (where applicable)
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, please refer to Q 5.10.
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, student & staff data (only) can be exported from ParentMail's system by the school.

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 ParentMail is likely to comply with the DPA in relation to data integrity ParentMail 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		We utilise Trustwave for regular monthly vulnerability and security scanning of our services. Monthly recommendation reports are provided by Trustwave and actioned accordingly and reported to the Board. Our hosted solution arrangements are ISO 27001 certified.

aspects of your service?		
Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers?		Upon written request, ParentMail will provide a confidential summary of the current monthly report.
Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards?		Yes, the audits are carried out under PCI DSS standards.
Q 6.4 – Are audit trails in place enabling users to monitor who is accessing their data?		Yes, extensive logs & audit trails are maintained.
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, daily backups are taken and are securely stored at our hosting facility. Remote/off-site backups are also taken.
Q 6.6 – Does your service have a		Yes, this plan is an internal document only.

disaster recovery plan, and is information on this plan made available to current/prospective cloud service customers?		

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 ParentMail 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 deliveries of the services is handled by multiple core database servers (load balanced) and separate multiple web servers (again load balanced). Each of these layers, database/web uses Virtual machine technology to automatically switch in additional software servers to cater for load conditions and failure. Failure of individual machines is handled automatically by the cluster management systems, automatically alerting ParentMail technical staff to issues. To combat loss of cloud connectivity our providers source internet services from multiple providers /backbones and also use power supplies from different utility companies to their locations. Coupled with on site generation capabilities there are clearly a number of levels of fall back. ▪ Loss of internet provider 1 – falls back to provider 2 ▪ Loss of provider 2 falls back to provider 3 ▪ Loss of electricity supplier 1 – falls back to provider 2 ▪ Loss of provider 2 – falls back to on site generation of electricity. ParentMail can therefore offer a 99.9% uptime service to its customers.

Q 7.2 – Does your service offer guaranteed service levels?		Yes, ParentMail offers a guaranteed uptime service of 99.9%. We ensure that all maintenance or enhancements are undertaken out of hours to prevent any disruption to schools.
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?		Yes, we have an established escalation procedure in the event of service levels not being met and for complaints. This is managed, recorded, tracked and reported through our Customer Relations Management software.

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, ParentMail has responded as follows:

Question	Supplier Response Code	Response Statement with Supporting Evidence (where applicable)
Q 8.1 – In providing the service do you limit the transfer of personal data to countries within the EEA?		Yes, only operate within the UK.
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?		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?		Yes, ParentMail from its inception has confirmed it will not provide advertising or similar through its service to customers.

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, as Q9.1 and our Privacy Policy.
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, as Q9.1 and our Privacy Policy.

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: ParentMail provides a fully manned Customer Support Team during office hours (01733 595962) and this should be the first point of contact in the event of a serious issue.

A serious or catastrophic issue would be escalated to the Operations Director to assist the school and ensure the required ParentMail resources are allocated to assist from Customer Support Advisors to our in-house IT Software Engineers

/Infrastructure Team and also our Social Media Team.

In many situations, a school is able to find an answer via our online self-help resources which include:

1) FAQs of common faults
2) Application and training guides
3) Training videos for all applications
4) WalkMes – Guided walk throughs of the key functions which can be accessed via the application and our main website

ParentMail provides support via telephone (01733 595962), e-mail (school_support@parentmail.co.uk) and online chat facility.

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: ParentMail has built in redundancy at the core of our system to help prevent serious incidents for our customers and we have achieved this in the following ways;

SMS and Email service failure

Automatic fail over and redundancy in our Email and SMS systems – should either primary systems fail we have queuing systems in place to automatically route to a fail over provider. This switch over does not require any user intervention. For example, we use three core suppliers for SMS, Primary O2, Secondary AQ Limited and tertiary Reach Data with instant fail over across these suppliers.

Hosting failures

Delivery of the service is handled by multiple core database servers (load balanced) and separate multiple web servers (again load balanced). All of these layers (database/web) uses Virtual machine technology to automatically switch in additional software servers to cater for load conditions or failure. Failure of individual machines is handled automatically by the cluster management systems, alerting ParentMail technical staff to any issues.

In the event of a total loss of hosting centre we are able to recreate the ParentMail environment within a 24-hour period.

Payment processing

Issues with Payment gateways are thankfully extremely rare, however, in the event of failure of our primary gateway (Pay360) the ParentMail system can utilise card processing from the PayPal platform with no interruption of service.

Loss of Head office

Should the main offices of ParentMail suffer flood/fire etc. and not be accessible we have ensured that all of our staff and systems can be accessible from a remote location. Our CRM database is cloud hosted (Salesforce.com) enabling our staff to access customer records and continue support. Our offices also use VOIP (Voice over Internet Protocol) telephony services enabling us to direct our calls to any alternative location with Internet access. This could be Directors houses or alternative temporary office locations if the access was to be restricted for prolonged periods.

Failure of internet connectivity

Issues arising in this area are really two fold.

Loss of core connectivity to the datacentre cloud that operates the ParentMail service and loss of connectivity from schools.

Failure of core Cloud connectivity

To combat loss of cloud connectivity our providers source internet services from multiple providers/backbones and also use power supplies from different utility companies to their locations. Coupled with on site generation capabilities there are clearly a number of levels of fall back.

- Loss of internet provider 1 – falls back to provider 2
- Loss of provider 2 falls back to provider 3
- Loss of electricity supplier 1 – falls back to provider 2
- Loss of provider 2 – falls back to on site generation of electricity.

Failure of local internet connectivity from school

Due to the way that the Internet is built communication will automatically route round breakages or congested areas. However, loss of direct internet connectivity from the school environment is not within our control and the school would need to manage the restoration of services directly with their supplier.

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 environment is certified to ISO 27001:2013

Cloud system access is through certificate based logins from a restricted white list of IP addresses.

Admin access to systems is restricted based on white list IP addresses and 2 factor authentication.

Helpdesk/security staff access is available through secure remote desktop sessions while client is present and viewing.

School side of ParentMail service is provided and maintained by a validated school user. This user, is responsible for the creation of school staff user accounts and their associated privileges, example access to e-mail, sms, payments, reports etc.

All access to ParentMail is restricted based on login ID and password and is encrypted.

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:

ParentMail inherently provides multiple data recovery solutions to schools in the

event of a data loss or deletion as follows:

1. An MIS link is available that extracts pupil and parent information in to ParentMail and this normally runs automatically on a daily basis. In the event of data deletion, this will repopulate ParentMail the next working day or can be instigated manually by the School themselves at any time.

   Time to fix – same day.

2. A backup and restore function is provided in our software and can be accessed and used by the ParentMail Administrator to restore not only their data but also their ParentMail user groups (used to differentiate pupils, classes, subjects, years etc).   *Time to fix – same day.*

3. ParentMail Support staff would ascertain the full impact of any loss of data including the order that events have occurred from conversing with school and examination of our extensive audit trails. Only when fully understood would data be restored to a point in time that is agreed with the school.

   Time to fix – typically 24 – 48 hours during business hours.

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: The school should contact the Customer Support Team to log the issue and for initial support. ParentMail would assist the school in identifying the potential cause and minimising the impact of the serious event. We would also assist in the preparation of communications by providing technical support and/or explanation of the cause.

We would also regularly monitor social media sites and the Social Media Team would assist in keeping the school advised of any significant attention and provide advice on handling any enquiries.

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: The school should contact the Customer Support Team to log the issue and for initial support. ParentMail would ensure that our in-house IT Software Engineers/Infrastructure Team were available to provide as much technical support as necessary to the school during this period.

ParentMail would assume that the school, as Data Controller, would be the correct party to contact the relevant authorities in the event of the school's system being hacked and pupil data compromised. Only in the event that ParentMail's wider systems are hacked, would we firstly inform the Data Protection Agency and then the affected schools whilst taking every possible action to defeat the hack and secure all systems.

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: The school should contact the Customer Support Team to log the issue and for initial support. ParentMail would ensure that our in-house IT Software Engineers/Infrastructure Team were available to provide as much technical support as necessary to the school during this period.

ParentMail would assist the school in the recovery of the lost or leaked data and in addition provide support in the preparation of any communications by providing technical support and/or explanation of the cause.