Cloud Software Services for Schools

Supplier self-certification statements with service and support commitments

Supplier name	GRC ONE Limited
Address	International House, St Katherine's Way, London. EW1 1YL
Contact name	Daren Martin
Contact email	daren.martin@grc1.com
Contact telephone	0333 344 8600

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 FDF Risk Manager and School Governance 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 Daren Martin 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 selfcertification 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, GRC ONE Limited confirms the position to be as follows for its FDF Risk Manager and School Governance services, fuller details of which can be found at www.GRC ONE.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.** Our standard contract allows any UK based organisation to meet the requirements applicable to it 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

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 subject to the jurisdiction of the English courts.
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.** Users have access to their own information from within the services. In addition, GRC ONE provides the Customer administrators with tools which may assist Customers with accessing and editing 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 GRC ONE Limited is likely to comply with the DPA in relation to data processing, GRC ONE 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?		**No.** GRC ONE does not act as the data controller. For some customers GRC ONE does supply example Risk and Governance data, however it is at the sole discretion of the organisation buying our service as to whether they use this data for organisation.
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.** GRC ONE only acts as a data store on behalf of our customers, however when and if we are required to make amendments to the data on behalf of our Customers we only act according to the emailed instructions of the Customers administrator.
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 standard terms and conditions incorporate our compliance agreement

		Yes. GRC ONE will only process customer data in accordance with the customer agreement and will not process Customer Data for any other purpose.
Q 4.4 – Is the processing of personal data or metadata limited to that necessary to deliver [or improve] the service?		
Q 4.5 – Where your contract does not cover every aspect of data processing, are you prepared to enter into a separate dataprocessing agreement with your cloud services customer?		**Yes.** If required GRC ONE will enter into an Amended Agreement

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 GRC ONE is likely to comply with UK law in relation to data confidentiality GRC ONE 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.** GRC ONE does not share any Customer data with any other service or party, irrespective of whether that service it is owned or not by GRC ONE Limited.
Q 5.2 – Do you prohibit personal data or metadata being shared with third parties?		**Yes.** GRC ONE does not share any Customer data with any other service or party.
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 encrypted via HTTPS (SSL). All passwords are hashed and encrypted.
Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?		**Yes.** Under normal circumstances only the Customers Administrator will add or edit the users account. GRC ONE Account Managers can request action by our support team on behalf of customers as long as these instructions are received in advance by email from the Customers administrator.

Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?		**Yes.** GRC ONE support staff only have access to the basic detail of the customer reference data. Our internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process personal data.
		Logins to customer reference file data is strictly controlled and passwords regularly changed.

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.** Our service is accessed over a HTTPS connection so communications between your browser and the website are encrypted.

Q 5.7 – Does your cloud service ensure that data at rest is encrypted?		**No.** Not all data within the core database is encrypted at rest, however we use MS Azure as our cloud service provider who's data security is second to none.
Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?		**Yes.** Our service is accessed over a HTTPS connection so communications between your browser and the website are encrypted regardless of whether you are accessing our services via desktop computed, laptop, tablet or smartphone.
Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?		GRC ONE does not provide email facilities, utilising the Microsoft email services resident with MS Azure.
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.** GRC ONE makes and retains a rolling 30 day backup regime, whereupon reaching the 30 days, the backups are overwritten. Upon cancellation of subscription, GRC ONE will delete the production copy of the customer's data within 30 days of being notified that the agreement is at an end.

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.** Upon cancellation of the subscription, GRC ONE will permanently delete the production copy of the customer's data within 30 days of being notified that the agreement is at an end.
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.** The Customers Administrator can export/download their data at any time

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 GRC ONE is likely to comply with the DPA in relation to data integrity GRC ONE 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**. Annually we have an independent CREST certified security consultancy conduct an audit\test of our service.
Q 6.2 – Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers?		**Yes.** Audit results can be made available to our Customers upon signing of an NDA, however as these are technical audits that con, they are summarised to both provide readable content and to protect our system security features.
Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards?		**Yes.** As previously stated, an independent CREST consultancy is engaged to conduct these tests. The audit is performed according to the internationally recognized ISO 27001 standard. Additionally the Microsoft Azure platform is are accredited by the UK Government for Official Data (see the CloudStore for details).
Q 6.4 – Are audit trails in place enabling users to monitor who is accessing their data?		**No**. There are audit trails within some parts of the system that are currently only accessible by our backend support staff. A user Audit Trail is within the development pipeline.

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.** As previously stated GRC ONE makes and retains a rolling 30 day backup regime, whereupon reaching the 30 days. In addition Microsoft's stores data our customer provide through use of Microsoft's cloud services in a redundant environment with robust backup, restore, and failover capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are implemented, ranging from redundant disks to guard against local disk failure, to continuous, full data replication to a geographically distant datacentre to reduce the impact of natural disasters.
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.** Our service does have a disaster recovery plan, however this information has not been made available to or requested by any current subscription 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 GRC ONE 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		**Yes.** We have selected MS Azure as our cloud datacentre service provider as their resilience and performance is second to none. Over the last 3 years we have had no planned downtime, running our service for in excess of 99.8% availability.
provide a resilient, reliable and accessible service at all times?		
Q 7.2 – Does your service offer guaranteed service levels?		**Yes.** We provide guaranteed customer support services between the hours of 8am and 6pm Monday to Friday UK Time and we aim to answer all queries within 1 hour of them being received. Our subscription service is available 365 days of the year, However we schedule major software releases at weekends and minor software updates overnight between the hours of 2am and 7am. For the most part, these releases should be invisible to our customers.
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?		**Yes.** Although service levels are not expected to be breached by GRC ONE or Microsoft Azure, GRC ONE can create a replacement service from back-up data, hosted with an alternative cloud provider within 48 hours if needed.

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 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.** All data is held in an EEA datacentre. No data is transferred out of the EEA
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?		
Q 8.3 – If you transfer data outside the EEA does your standard contract include the unmodified EU approved “model clauses” in respect of such transfers?		n/a

Q 8.4 – If you transfer data outside the EEA, (and do not offer the unmodified EU approved "model clauses", can you confirm that the requirements of the DPA are met in respect of the need for adequate protection for the rights and freedoms of data subjects in connection with the cross-border transfer and processing of their personal data?	[redacted]	n/a

9. Supplier Response - Use of Advertising

Recognising the particularly sensitive nature of the data likely to be processed in a cloud service aimed at schools, there is particular concern in relation to the use of advertising and the extent of data mining which providers of cloudbased 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.** GRC ONE services are supplied free from advertising of any kind.

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.** GRC ONE does not mine any data within its services for advertising or any other purpose other than to check the customer's current usage and subscription status.
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 is provided as terms within our existing standard contract.

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: Serious issues should be reported immediately to support@grc1.com or through the website using the support link. Email support is available outside of hours, however will be responded to within 1 hour between 8am and 6pm Monday to Friday.
In addition, customer administrators can make contact with us on +44 (0) 333 344 8600 Monday to Friday, 8am-6pm. In a severe scenario, onsite support can be arranged.

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: GRC ONE will do everything that is reasonably possible to resolve a serious incident within 1 hour of being notified. In the event of a serious incident, GRC ONE will set up an emergency support team, with a dedicated contact for the schools affected. In a severe scenario, onsite support can be arranged. First contact should be made to support@grc1.com by the customer's administrator. In addition, customer administrators can make contact with us on +44 (0) 333 344 8600 Monday to Friday, 8am-6pm.

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:

N/A - GRC ONE is a browser based software as a service solution, so there is no need for any additional configuration. Our software is built and tested to run on the latest copies of browsers

GRC ONE does not hold business critical data (although data is classified as sensitive and confidential).

Password policies change as security vulnerabilities are responded to, however the latest password requirements are clearly detailed within the system's password screens and training documentation.

At the time of filling in this self-assessment the password rules are that a password must be :

- Between 8 and 14 characters in length

Contain a minimum of

- 1 uppercase alpha character
- 1 lower case alpha character
- 1 numeric or 1 special character

You cannot have a numeric or alpha run of more than 3 characters (e.g. abc, 123) and must not contain the users name or any common word.

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 previously communicated we can restore a customer's data up any end of day in the last 30 days from the current date.

First contact should be made to support@grc1.com by the customer's administrator.

In addition, customer administrators can make contact with us on +44 (0) 333 344 8600 Monday to Friday, 8am-6pm.

GRC ONE will endeavour to recover data within the first 24 hour period following a request.

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:

GRC ONE will not comment on or provide any information to the press regarding their service or a subscribing customer without the express consent of the customer involved.

GRC ONE CEO and COO will work with any school that requires the managing of media attention ascertaining to our product/s.

First contact should be made to support@grc1.com by the customer's administrator.

In addition, customer administrators can make contact with us on +44 (0) 333 344 8600 Monday to Friday, 8am-6pm.

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:

GRC ONE does not carry or hold any personal data regarding individual pupils or staff, however if requested to do so, senior members of GRC ONE Education team will work

with the school or relevant agencies to provide clear precise answers and assistance wherever possible.

First contact should be made to support@grc1.com by the customer's administrator.

In addition, customer administrators can make contact with us on +44 (0) 333 344 8600 Monday to Friday, 8am-6pm.

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:

Senior members of GRC ONE Education team will work with the local authority and or agencies to provide clear precise answers and assistance wherever possible.

First contact should be made to support@grc1.com by the customer's administrator.

In addition, customer administrators can make contact with us on +44 (0) 333 344 8600 Monday to Friday, 8am-6pm.