Cloud Software Services for Schools

Supplier self-certification statements with service and support commitments

Supplier name	Microsoft Limited
Address	Thames Valley Park, Reading, RG6 1WG
Contact	UKEdu@Microsoft.com

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 Microsoft 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 Beswick, UK Education Director** 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, Microsoft confirms the position to be as follows for its Office 365 and Microsoft Azure service, fuller details of which can be found at the Office 365 Trust Centre and Microsoft Azure Trust Centre:

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** - Consistent with the DPA, Microsoft offers a written contract that requires Microsoft: "*will only act upon customer's instructions," (ii) has implemented measures to protect customer data against improper access, disclosure, or, loss, and (iii) will comply with all applicable 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?		*Not applicable, our standard contracts are consistent with the DPA.*

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** - Microsoft's contract is enforceable in Ireland and the EU Model Clauses will be enforceable in the UK. Microsoft must bring any actions against UK customers in the UK.
Q 3.4 – Do your services ensure that schools are able to comply with their obligations with regard to the exercise of data subjects' rights?		**YES** - Microsoft's agreement obligates it to support the exercise of data subjects' rights. Administrative tools are provided to Microsoft's customers, enabling them to address data subject requests to correct, delete, or block 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 Microsoft is likely to comply with the DPA in relation to data processing, Microsoft 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?		**YES** - For cloud services, Microsoft is a **data processor** acting on behalf of its customer. The only exception is that Microsoft is a data controller for customer account information (e.g. billing information, administrator information).
Q 4.2 – Where you act as a data processor does your contract ensure that you will only act on the instructions of the data controller?		**YES** - Microsoft's contract for cloud services explicitly state that ""*Microsoft will only act upon Customer's instructions*." Microsoft's contract with the customer are customer's complete and final instructions to Microsoft for the processing of customer data.
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** - Microsoft's agreements detail the specific security measures we implement and maintain to protect customer data. These measures meet or exceed those imposed upon data controllers in the UK through the DPA's Seventh Principle.

Q 4.4 – Is the processing of personal data or metadata limited to that necessary to deliver [or improve] the service?		**YES** - Microsoft commits that it will only use data our customer provides us through use of our cloud services "*to provide"* those services and for *"purposes consistent with providing"* those services.
Q 4.5 – Where your contract does not cover every aspect of data processing, are you prepared to enter into a separate data-processing agreement with your cloud services customer?		*Not relevant - Microsoft's contracts for cloud computing and services cover every relevant aspect 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 Microsoft is likely to comply with UK law in relation to data confidentiality Microsoft 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** - Microsoft expressly commits that it will only use data our customer provides us through use of our cloud services for purposes consistent with providing those cloud services.
Q 5.2 – Do you prohibit personal data or metadata being shared with third parties?		**YES** - Microsoft only shares data our customer provides through use of our cloud services with those affiliates and subcontractors that we use to provide the services. Customers can find a list of these third parties here for Office 365 and here for Microsoft Azure.

Q 5.3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts?		**YES** – Microsoft's cloud services allow various options such as federation, multi-factor authentication and secure password synchronization to ensure that users are authenticated into the cloud service in a secure manner. Full details of Microsoft's approach to security can be found in our Security White Papers referenced here for Office 365 and here for Microsoft Azure.
Q 5.4 – Does your service have in place arrangements to assist schools in protecting access to personal data and/or user accounts?		**YES** - In addition to enabling multi-factor authentication, Microsoft's cloud services also include malware protection, and administrative controls to help schools protect access to data and accounts.
Q 5.5 – Are appropriate controls in place to ensure only authorised staff have access to client/customer data?		**YES** - Microsoft expressly commits that we restrict access to customer data to only those individuals "*who require such access to perform their job 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** - Microsoft encrypts, or enables our customer to encrypt, data that customers provide us that is transmitted over public networks.
Q 5.7 – Does your cloud service ensure that data at rest is encrypted?		**YES** - Email and SharePoint Online content is stored on servers protected with Microsoft's BitLocker encryption for data at rest. Additionally, Microsoft offers a number of encryption options to customer administrators of its cloud services. Windows Azure customers may encrypt data at rest via Windows Azure's encryption APIs.

Q 5.8 – Does your cloud service ensure that data in transit between your data centres is encrypted?		**YES** - All transfers between data centres over the public Internet are encrypted. Furthermore all data transmissions between Microsoft data centres utilising Microsoft private lines will be encrypted during 2014.
Q 5.9 – Does your cloud service ensure that email traffic between your cloud service and other cloud service providers can be encrypted?		**YES** – Microsoft provides options for administrators to select Forced TLS or Opportunistic TLS to encrypt email traffic between Microsoft's cloud services and other cloud service 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** - Microsoft commits to delete customer's data provided through use of our cloud services no later than 180 days after (i) contract end, or (ii) the customer marks the data for deletion.
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** - Microsoft's commitment stated in Q5.10 applies to all the data our customer provides us through use of Microsoft's cloud services.
Q 5.12 – Does your service provide a mechanism free of charge whereby users		**YES** - Microsoft's customers may download their data at any time, without charge, and without any assistance from Microsoft. Additionally, Microsoft provides tools (without additional charge) to

can access a complete and secure copy of their data?		help customer administrators provide individual users with access to their data.

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 Microsoft is likely to comply with the DPA in relation to data integrity Microsoft 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** - An independent third party audits the security of the computers and computing environment that it uses in processing data our customer provides Microsoft through use of Microsoft’s cloud services and the physical data centres from which Microsoft provides the services. This audit is performed at least annually by qualified, independent security professionals.
Q 6.2 – Where the above audits are conducted, do you make the findings		**YES** - Upon written request, Microsoft will provide our customer with a confidential summary of the report resulting from the audit referenced in Q6.1. The summary report will clearly disclose the scope of the audit and any material findings by the auditor.

available to current and/or prospective cloud customers?		
Q 6.3 – Does your service ensure that where such audits are carried out, they are conducted to best industry standards?		**YES** - The audit referenced in Q6.1 is performed according to the internationally recognized ISO 27001 standard. Additionally Office 365 and Microsoft Azure 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?		**YES** - Customer administrators are able to view access logs of individual user accounts.
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** - 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** - Microsoft maintains emergency and contingency plans for the service facilities, a high level summary of Microsoft's approach to service continuity can be found here for Office 365 and here for Windows Azure.

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 Microsoft 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** - Microsoft's investments in high-capacity data centres throughout the world, and it's innovations in cloud infrastructure and architecture ensure that its cloud services are highly scalable and can support everything from a one-person business to companies with tens of thousands of users.

Q 7.2 – Does your service offer guaranteed service levels?		**YES** - Microsoft's cloud services provide financially backed service level agreements. See the Service Level Agreement for Microsoft Online Services and the Windows Azure Service Level Agreement for more information.
Q 7.3 – Does your service provide remedies to customers in the event that service levels are not met?		**YES** - Microsoft's cloud services provide financially backed service level agreements that provide compensation to customers for outages that exceed the committed service level.

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, Microsoft 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?		Microsoft will store data our UK customers provide through use of Microsoft's cloud services in our European data centres in Ireland and the Netherlands. There are limited circumstances, such as to provide customer and technical support that would cause transfers of European customers' data outside of the EEA.
Q 8.2 – If you transfer data outside the EEA do you explain to schools when (and under what circumstances) data will be transferred to these locations?		**YES** - Microsoft's cloud services have web-based trust centres that provide a clear description of where the customer data will be stored. Customers can find details here for Office 365 and here for Microsoft Azure.

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?		**YES** - Microsoft was the first large cloud provider to offer the EU Model Clauses to all of its customers. Microsoft’s utilisation of the EU Model Clauses has been recently endorsed as compliant with EU data protection laws by the Article 29 Working Party, the EU’s collection of data protection authorities.
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?		*Not Applicable, Microsoft utilises the EU Model Clauses.*

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** - Microsoft has made a longstanding commitment that it will not use data Microsoft's customers provide us through use of our cloud services for any advertising or similar commercial purposes.

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** - Microsoft makes a contractual commitment not to use any information derived from data our customer provides us through use of our cloud services for any advertising or similar commercial purposes.
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** - Microsoft will not use data our customer provides us through use of our cloud services or derive information from it for any advertising or similar commercial purposes, and will not sell data customers provide us through use of our cloud services.

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: If a school has any Support, Data Protection or Privacy issues with Office 365 services it is important to always register a support call with the free Office 365 support service. Formally registering a call will ensure that a Support Request number is issued and that progress and escalation can be tracked, monitored and audited. A call can be raised using the support link in the Office 365 Administration portal or by calling the UK Based Freephone number – 0800 032 6417 or 0203 450 6455 (local call charges

apply). Free Technical support via the online call registration and phone number is provided 24x7.

Always state the nature and severity of the issue. If an issue is regarding Data Protection and or Privacy, please clearly state this, as a separate process will be initiated by the support team.

If at any time you feel a call is not being responded to in a timely or appropriate manner, please escalate to UKEducation@Microsoft.com please include the Service Request number (you will receive a Service Request Number when you log call) and a brief description of the issue. This is a group email address that includes Microsoft Employees who belong to the UK Microsoft Education team. A member of the Schools team will respond.

If you have worked with a local Microsoft partner in setting up your Office 365 School environment, it is always advised to contact them. They will also be able to escalate a call on your behalf. Subject to any terms you may have agreed with a local Microsoft Partner, you may also be able to call in on-site support directly from your partner.

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 free, 24x7 support for Office 365, along with its processes for management, escalation and auditability is designed to handle all types of issues, from technical to Data Protection and Privacy concerns. To ensure proper tracking and escalation it is highly recommended to log a support call. This will give the school access to formal support mechanisms designed to address the type of issue or incident being experienced.

If a School is concerned that a Security, Data Protection or Privacy issue is not being addressed in a timely or an appropriate manner then Microsoft UK has also provided an escalation route using an email alias that includes members of the UK Microsoft Education team. UKEducation@Microsoft.com When using this, please include your service request number (SR), severity of your issue and a brief description. Dependant on the issue, a member of the UK Education team will respond and engage to resolution.

3.3 SOLUTION CONFIGURATION.

Whilst virtually all cloud service providers have detailed technical advice on how their systems should be configured, this section of the supplier response should set out the general principles which school management should expect to see implemented to ensure maximum security of their cloud implementation.

This might cover for example:

- The need for correct configuration of access devices
- The use of additional backup / data synchronisation arrangements for sensitive or business critical data
- Configuration options or additional services that provide greater level of security than is available in your free offering
- Sample password policies in relation to the age and ability of the users of their service
- Policies in respect of helpdesk and security staff access to client data

Supplier response:

Office 365 provides an Enterprise class platform for School Collaboration and productivity. The Office 365 services are modular by design giving schools complete flexibility in terms of choice, configuration and customisation of the services. The links below provide access to guidelines in creating and configuring Office 365 for Schools including optional security enhancements.

The Office 365 platform includes the following services for schools use:

- Email and Calendaring service – Microsoft Exchange Online (50Gb mailbox per person)
- Staff and student personal file storage area (1Tb per person)
- Teacher, class, clubs, special interest and school management shared areas
- Instant Messaging, audio and high definition video conferencing for up to 200 people per conference call – integrated with Calendaring
- Remote desktop control
- Internal facing webpages
- One external facing webpage
- External access for parents (requires configuration)
- Social networking environment
- Online access to (browser based) Word, Excel, PowerPoint and OneNote
- Full Client Office Professional suite for pupils for up to 5 devices (including iPads®) at no *cost

All the above Office 365 modules are provided at no cost for schools

*Subject to conditions. Get Office Professional full client suite (the full client version) for your students at no additional cost when you have Microsoft Office

licensed for faculty and staff. Please contact your license provider to verify eligibility.

Signing up for Office 365

Try Office 365 free and see how it can help your school. Here's how:

1. Sign up for a free trial. Explore the features and benefits of Office 365 for up to 50 users. Please follow the link below and click on the 'Free 30-day trial' http://office.microsoft.com/en-gb/academic/compare-office-365-education-plans-FX103045755.aspx
2. Verify eligibility. At any time during the trial you can have Microsoft verify your domain's eligibility for academic prices. The Office 365 for Education Plan A2 plan provides all of the above listed modules at no cost to the school
3. Start using the service. Deploy the free service (Office 365 for education Plan A2) to your entire school.

To qualify for Office 365 for education you must be an accredited educational institution. You will be required to sign a contract and attest that you are an eligible customer. Microsoft reserves the right to verify eligibility at any time and suspend the service for ineligible customers.

Further resources

Microsoft in Education - Office 365 resources This link provides further information on Office 365, training and a 'Next steps' guide in signing up and deploying Office 365 for your school. The 'Next steps' links provide further information on how to:

1. Start your free trial today
2. Get Ready to deploy
3. Learn how to use

Office 365 Education Starter Manual for Schools. Whitepaper guide on how to configure Office 365 for schools

Office 365 Deployment Guide for IT Professionals.Specialist technical guide and instruction for School IT staff

Introduction to Office 365 – Online Training

Office 365 Fasttrack Pilot – Online Training

Help for teachers in using Office 365 in the classroom

Enhanced Security services for Office 365

Please click on the information links below for more information on enhanced security options

Multifactor Authentication – Providing 2 forms of authentication (Password and onetime use telephone passcode)

Encrypted emails (note this is a chargeable service) – Send encrypted emails to other staff or to people outside of School contacts

Data Loss Prevention (note this is a chargeable service) – Stop sensitive information from leaving the school

Information Rights Management (note this is a chargeable service) - Applying security at the document level

Guide for creating Pupil Supervision Policies in the eMail service

Office 365 (Azure Active Directory) Password Policy

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:
Individuals and or School Office 365 administrators using the school Office 365 environment can restore emails, folders and email boxes for up to 30 days after deletion. School Office 365 Administrators can recover files for a further 14 days after the 30 day period has lapsed.

Individuals and or School Office 365 administrators can recover deleted Files and folders up to 90 days after deletion. Revision copies and version control can be configured for file storage areas to ensure copies are made for each document that is edited.

If a school experiences loss of data that can't be recovered by local School Office 365 administrators it is important to register a support call with the free Office 365 support service. Formally registering a call will ensure that a Support Request number is issued and that progress and escalation can be tracked, monitored and audited. A call can be raised using the support link in the Office 365 Administration portal or by calling the UK Based Freephone number – 0800 032 6417 or 0203 450 6455 (local call charges apply). Free Technical support via the online call registration and phone number is provided 24x7.

Depending on the circumstances and issue file recovery can be completed within a day of making a support call. Longer recovery times can be experienced depending on the nature of the issue.

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:
If a school experiences a serious incident with Office 365 services it is important to always register a support call with the free Office 365 support service. Formally registering a call will ensure that a Support Request number is issued and that progress and escalation can be tracked, monitored and audited. A call can be raised using the support link in the Office 365 Administration portal or by calling the UK Based Freephone number – 0800 032 6417 or 0203 450 6455 (local call charges apply). Technical support via the online call registration and phone number is provided 24x7. State the severity of the incident and the wider community involved.

In addition to registering a support call, contact Microsoft UK using the UKEdu@Microsoft.com alias. State the severity of the incident and that local and or National media are involved. Senior members of the Education team will reach out to the school(s) to assess the incident and, if necessary, engage directly to assist in managing the media to resolution.

In this case it would also be advisable to engage with your Local authority for guidance and advice.

3.6 ENGAGING WITH CHILD SUPPORT AGENCIES

Where a serious event had resulted in issues being raised that related to child protection – for example the loss of sensitive pupil data, the cloud service provider should indicate what it would do to assist the school in engaging with the relevant child protection agencies, over and above the contractual minimum.

Supplier response:
If a school experiences an issue related to child protection with Office 365 services it is important to always register a support call with the free Office 365 support service. Formally registering a call will ensure that a Support Request number is issued and that progress and escalation can be tracked, monitored and audited. Please state that the issue is regarding privacy and child protection incident. This will trigger a different process than a standard support call.

A call can be raised using the support link in the Office 365 Administration portal or by calling the UK Based Freephone number – 0800 032 6417 or 0203 450 6455 (local call charges apply). Technical support via the online call registration and phone number is provided 24x7. State the severity of the incident and the wider community involved.

Contact Microsoft UK using the UKEdu@Microsoft.com alias. Microsoft UK Education Team members belong to this alias. State the severity of the incident. Senior members of the Education team will reach out to the schools to assess the incident and as necessary engage directly to resolution.

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:
If a school experiences a serious incident with Office 365 services it is important to always register a support call with the free Office 365 support service. Formally registering a call will ensure that a Support Request number is issued and that progress and escalation can be tracked, monitored and audited. A call can be raised using the support link in the Office 365 Administration portal or by calling the UK Based Freephone number – 0800 032 6417 or 0203 450 6455 (local call charges apply). Technical support via the online call registration and phone number is provided 24x7. State the severity of the incident and the wider community involved.

Contact Microsoft UK using the UKEdu@Microsoft.com alias. Microsoft UK Education Team members belong to this alias. State the severity of the incident. Senior members of the Education team will reach out to the schools to assess the incident and as necessary engage directly to resolution.