SOUTH WEST GRID FOR LEARNING

SOUTH WEST TEACHER NETWORK

Guidance for schools: **Cloud hosted services**

Are you considering using products and services that are hosted in the cloud? This document is designed to help you to understand your obligations and help you establish the appropriate policies and procedures when considering switching from locally-hosted services to cloud-hosted services.

For many schools, the initial change from ‘local’ to ‘cloud’ takes place in relation to email services; much of this guidance is applicable to cloud services in general, while some particular areas focus on email.

What are schools’ legal obligations?

All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

Schools, like any other organisation, are subject to the Data Protection Act (DPA) and its eight basic principles. The DPA refers to ‘personal data’ - this can be described generally as information which identifies an individual and is personal to an individual. The DPA contains eight “Data Protection Principles” which specify that personal data must be:

- Processed fairly and lawfully;
- Obtained for specified and lawful purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept any longer than necessary;
- Processed in accordance with the “data subject’s” (the individual’s) rights;
- Securely kept; and
- Not transferred to any other country without adequate protection in situ.

It’s also worth considering that whilst not all data is “personal”, that which is has varying levels of sensitivity based on the impact were it to be compromised.

The Information Commissioners Office has produced a report, in plain English, aimed at helping schools meet their data protection obligations; you can read the report detailing data protection advice for schools here and a simple summary of the report here.

But what does this actually mean in practical terms and what should you be looking out for when considering the switch to cloud-based services?

How long must the email data be retained (archived) by the school? And when should the school remove archives?

E-mail is primarily a communications tool, and many cloud email applications are not designed for the secure long term storage of what could be sensitive data.

E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? Schools should retain copies of such emails according to their importance or sensitivity and this must correspond with the schools retention schedule and existing security practices. These emails may need to be regularly and systematically saved into a local secure storage system with appropriate backup routines or printed out and filed in the same way as other sensitive paper documents.

Where can the data be stored? And where can't the data be stored?

The DPA (Principle 8) states that personal data must not be transferred to any other country without adequate protection in situ[1]. Countries in the EU approach privacy protection differently to those outside; the US-EU Safe Harbour Framework bridges the gap between and enables US organisations to comply with the EU enhanced privacy protection.

So check carefully to see if your email is hosted within the EU or if it is hosted in the US, look out for the Safe Harbour Framework. It is worth noting that the Safe Harbour Framework is a self-regulated code of practice and not regulated by any legislation.

What security must the school put in place for the stored data?

Information security is a very important area for schools to get right.

Whilst unauthorised access or the loss of personal information can impact on the safeguarding of pupils, parents or staff, it can also have a significant impact on the reputation of the school and its leaders. In fact, the Information Commissioners Office now has the power to issue fines for serious breaches of the data protection principles. Find out more here.

As a general, common sense rule, schools should consider whether the data is personal, sensitive or may later be challenged. The kind of data which may attract challenge should attract extra security and schools may elect to keep this data within the school, or an alternative, secure system. The ICO suggests that schools should encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen. The kind of security for data envisaged by the Information Commissioners Office can be found here.

Only genuinely sensitive data needs to be safeguarded; the Government Protective Marking System here is part of the new 'Security Policy Framework[2]' and is a helpful source of information when considering the type of material that should be handled securely.

Consider when transferring information via email whether the email should be handled securely (i.e. encrypted). Ensure all staff are aware of the limitations of what data can be transferred or stored within cloud services and educate all users to enable them to identify sensitive personal data with a high impact level and to choose more secure transfer protocols. Unlike password protection, encryption is the only real secure method of transferring information via email. If you are a school in the South West, SWGfL is developing an approach for secure email to use for this purpose; contact sis@swgfl.org.uk for more information.

[1] Data Protection Act, Principle 8, Information Commissioners Office, http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx

[2] Protective marking of information is covered particularly in paragraphs 28 to 39 (pages 20 to 25)

Ensure good practise when sending email, taking extra care to ensure that you send to the right recipient(s). Many systems have auto-complete functions; make sure you choose the right address or recipient before you click send. Be careful when using a group email address; check who is in the group and double check that you really want to send your message to everyone. Remember that recipients who are carbon copied (cc) into an email can see one another's email addresses; use blind carbon copy (bcc) if you do not wish to reveal the email addresses to all recipients.

What policies and procedures should be put in place for individual users of cloud-based services?

The school is ultimately responsible for the contract with the provider of the system, so check the terms and conditions carefully; we've included a list of questions that you may want to consider when selecting an external email provider; indeed you may want to contact any potential provider and ask them for responses to each of the following:

- How often is the data backed up?
- Does the service provider have a clear process for you to recover data?
- Who owns the data that you store on the platform?
- How does the service provider protect your privacy?
- Who has access to the data?
- Is personal information shared with anyone else? Look out for opt in/opt out features
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that your information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification
- How will your data be protected? Look out for features that will keep your information safe and secure including Anti-spam, Anti-Virus and Anti-malware…
- How reliable is the system? Look out for availability guarantees.
- What level of support is offered as part of the service? Look out for online and telephone support, service guarantees

These questions are a great starting point for considering wider cloud based services. To save you time and effort we've teamed up with Microsoft and Google who have already answered these questions for Microsoft Office365 and Google Apps for Education[3].

South West Grid for Learning wishes to thank both Microsoft and Google for compiling their responses to each of the following questions.

[3] Correct at time of publishing (January 2013)

Microsoft® Office 365

Where is the data stored?

Data for UK Schools is all hosted within the EU. The primary Microsoft data centre we host the service in is located in Dublin and the fail-over is to Amsterdam.

How often is the data backed up?

The idea of “back up” is very different with Office365 than with traditional locally hosted services. We use a network of globally redundant data centres and replicate data on multiple servers across the two data centres. Any one time we keep 3 copies of schools data across the two data-centres mentioned (Dublin & Amsterdam).

Does the email service provider have a clear process for recovering data?

Yes. Users themselves can recover data for 30 days after deleting an item. Administrators then have a further 30 days once the item is deleted from the deleted-items folder. There are also additional paid-for archiving services available with Office365, but with a 25GB inbox per person the pressure on users to archive email is not as great compared to existing email systems.

How does the email provider protect your privacy?

3 key things: No advertising, no “mingling” of Office 365 data with our consumer services (such as Hotmail) and full data-portability, in case you ever want to leave the service. You can find lots more detail here

Who owns the data that you store on the email platform?

Schools own the data. Microsoft does not. You own your data, and retain all rights, title and interest in the data you store with Office 365. You can download a copy of all of your data at any time and for any reason, without any assistance from Microsoft.

Who has access to the data?

By default no one has access to customer data within the Office 365 service. Microsoft employees who have completed appropriate background checks and have justified need can raise an escalation for time-limited access to Customer data. Access is regularly audited, logged and verified through the ISO 27001 Certification.

As detailed in a recent accreditation submission to the UK Government, any organisation that specify “UK” as their country during tenant creation will be provisioned and data stored within the EU datacenters (Dublin and Amsterdam).

Microsoft has been granted accreditation up to and including the UK government’s “Impact Level 2” (IL2) assurance for Office 365. As of February 2013 Microsoft are the only major international public cloud service provider to have achieved this level of accreditation and, indeed, it is the highest level of accreditation possible with services hosted outside of the UK (but inside of the EEA).

Schools may wish to consider the extent to which applicable laws in the US – which apply to services operated by companies registered in the US, e.g. Microsoft and Google – affect the suitability of these services. For example the US Patriot Act provides a legal means through which law enforcement agencies can access data held within these services without necessarily needing the consent or even the knowledge of the customer. Whilst SWGfL doesn't intend to put anyone off getting value from these beneficial services we feel it's only right to share what we know about them.

Is personal information shared with anyone else?

No personal information is shared.

Does the email provider share email addresses with third party advertisers? Or serve users with ads?

No. There is no advertising in Office365.

What steps does the email provider take to ensure that your information is secure?

Microsoft uses 5 layers of security - data, application, host, network and physical. You can read about this in a lot more detail here

Office365 is certified for ISO 27001, one of the best security benchmarks available across the world. Office 365 was the first major business productivity public cloud service to have implemented the rigorous set of physical, logical, process and management controls defined by ISO 27001.

EU Model Clauses. In addition to EU Safe Harbor, Office 365 is the first major business productivity public cloud service provider to sign the standard contractual clauses created by the European Union ("EU Model Clauses") with all customers. EU Model Clauses address international transfer of data. Visit here to get a signed copy of the EU Model Clauses from Microsoft.

Data Processing Agreement. Microsoft offers a comprehensive standard Data Processing Agreement (DPA) to all customers. DPA addresses privacy, security and handling of customer data. Our standard Data Processing Agreement enables customers to comply with their local regulations. Visit here to get a signed copy of the DPA.

How reliable is the email service?

There is a 99.9% uptime commitment with financially-backed SLA for any paid-for services in Office365 (though most schools will be using 'free' services and therefore will not receive the financially backed SLA).

What level of support is offered as part of the service?

Microsoft offer schools direct telephone support 24/7 for IT administrators and there is also a large range of online help services, which you can read about here. Our recommendation is that schools use a Microsoft partner or support organisation with industry specific expertise in cloud services for schools.

Additional Resources

There is a wealth of information about Office365 in the Office365 Trust Centre. You can also read articles about Office365, get deployment resources and contact Microsoft Cloud experts direct on their UK Schools Cloud Blog.

Google Apps for Education

Unless stated, the answers work for both standard and offline agreements.

Where is the data stored?

Google maintains a number of geographically distributed data centers across the US and abroad. Information on our data centers can be found at: http://www.google.com/about/datacenters/locations/index.html

Google will store data in physically secure data centers, maintain data on Google-owned servers, and replicate Apps data across multiple systems within a single data center as well as back up data in a Google-owned secondary data center which will be in a different geographic disaster area from the first. Take a look data centre set up and security features to find out more.

Google Apps data is processed in accordance with the EU Directive and under the Safe Harbour Framework. We also have security certifications, such as the ISO 27001 and ISAE/SSAE certifications which prove the safety and security of our products. For more information take a look at the Google Apps security whitepaper and the Security FAQs

At the beginning of 2013 Google implemented new model contract clauses designed to act as an additional means of compliance with the European Commission's Data Protection Directive for Google Apps customers who operate within Europe, find out more here

How often is the data backed up?

Google replicate Apps data across multiple systems within a single data center as well as back up data in a Google-owned secondary data center which will be in a different geographic disaster area from the first.

Does the email service provider have a clear process for recovering data?

If a user has moved a message to Trash it will remain there for 30 days before being permanently deleted. During this time, the user can recover emails from their Trash. After this time, the email will be permanently deleted. Once an administrator or end-user has **permanently** deleted any data in Google Apps, we delete it according to your Customer Agreement and our Privacy Policy. Data is irretrievable once an administrator deletes a user account. If you need to recover email messages, Google offers additional archiving products that can complement Google Apps for Business, Government and Education editions. An administrator can also suspend rather than delete a user to retain all data associated with that account, while also blocking access to this account. The Client's data will reside in at least two Google data centers. Our Data Centers are redundant and can shift to a user's secondary data center. To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Google implemented comprehensive disaster recovery program at all of its data centers. This program includes multiple components to eliminate single point of- failure.

How does the email provider protect your privacy?

- Google Apps security whitepaper

- Review of Google Certifications, such as the ISO 27001 and ISAE/SSAE certifications

- Security FAQs

Who owns the data that you store on the email platform?

The customer is the owner of all content for their user accounts.

Who has access to the data?

Access to data is strictly controlled. Authorised staff have background checks performed on them, and have their activity strictly monitored. They only receive access to data on a need-to-know basis, for example, a Gmail support agent will be able to access Gmail data if you contact the support team asking for assistance. Google Apps has received a satisfactory SAS 70 type II audit. This means that an independent auditor has examined the controls protecting the data in Google Apps (including logical security, privacy, Data Center security, etc) and provided assurance that these controls are in place and operating effectively.

Schools may wish to consider the extent to which applicable laws in the US – which apply to services operated by companies registered in the US, e.g. Microsoft and Google – affect the suitability of these services. For example the US Patriot Act provides a legal means through which law enforcement agencies can access data held within these services without necessarily needing the consent or even the knowledge of the customer. Whilst SWGfL doesn't intend to put anyone off getting value from these beneficial services we feel it's only right to share what we know about them.

Is personal information shared with anyone else?

The data which you put into our systems is yours, and we believe it should stay that way. We think that means three key things.

- We won't share your data with others except as noted in our Privacy Policy.
- We keep your data as long as you require us to keep it.
- Finally, you should be able to take your data with you if you choose to use external services in conjunction with Google Apps or stop using our services altogether.

Google does not share or reveal private user content such as email or personal information with third parties except as required by law, on request by a user or system administrator, or to protect our systems. These exceptions include requests by users that Google's support staff access their email messages in order to diagnose problems; when Google is required by law to do so; and when we are compelled to disclose personal information because we reasonably believe it's necessary in order to protect the rights, property or safety of Google, its users and the public. Google complies with valid legal processes seeking account information, such as search warrants, court orders, or subpoenas. We attempt to notify users before turning over their data whenever possible and legally permissible.

What are the school obligations with regards use?

Schools are responsible for obtaining parental consent for the use of Google Apps for Education services. http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent'.

Normally, schools will incorporate this into their standard internet consent forms sent to parents each year. We would encourage schools to know and understand the security features that they can implement to protect younger users such as walled garden, turning on/off services by Org Unit, YouTube for Schools and objectionable content filters. Your school should familiarise itself with the general security features of Apps. Once the school has investigated all the child protection possibilities then they should be able to answer any parent's questions and/or create their own information sites (like two schools have done here and here) which gives information to address the concerns of parents and the steps that they are taking to protect the children using Google Apps within the school. See some of Google's suggested template letters for parents which should also help you understand how other schools deal with this.

Does the email provider share email addresses with third party advertisers? Or serve users with ads?

No

What steps does the email provider take to ensure that your information is secure?

- Google Apps security whitepaper
- Review of Google Certifications, such as the ISO 27001 and ISAE/SSAE certifications
- Security FAQs

How reliable is the email service?

We have a Service Level Agreement which guarantees that the services will be available 99.9% of the time. Google Apps has NO scheduled downtime, which is very unique. See our SLA here.

What level of support is offered as part of the service?

24/7 phone and email support for all Apps for Education customers. Only administrators of a domain can contact the support team, but a school can have multiple administrators. Administrators will have a unique pin number which they can use to contact the support team. See more here.

For more general information about Google Apps for Education please refer to the FAQ here