Godolphin

Data Protection Policy
(incorporating Personal Data Handling)

Reviewed in: June 2017 (v4)
Review in: June 2018
Reviewed by: Deputy Head Communication and Innovation, Senior Deputy Head, Head of ICT Services, Head

Refer also to the following policies:

Online Safety 1. Online Safety Policy
Online Safety 2. Acceptable Use Agreements
Online Safety 3. Technical Security Policy
Online Safety 5. Social Media Code of Practice
Online Safety 6. Online Safety Committee Terms of Reference
Online Safety 9. Privacy Notices

Table of Contents

Data Protection Policy
(incorporating Personal Data Handling)

Introduction

The Data Protection Act 1998 (DPA) lays down a set of rules for processing of personal data (both structured manual records and digital records) held by the School. It provides certain individuals (data subjects) with rights of access and correction. It also requires the School as a data controller to comply with eight data protection principles, which, among others, require the School to be open about how the personal data it collects is used.

This policy brings together the legal requirements contained in the DPA and all other relevant legislation, regulations and guidance and incorporates those eight principles. It applies to all forms of personal data held by the School, whether on paper or in electronic format, and it forms part of the School's online safety policy.

Anyone who has access to data of a personal or sensitive nature held by the School must know, understand and adhere to this policy and do everything within their power to ensure the safety and security of that material.

It is the responsibility of all members of the School community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the School into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office for the School and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Policy Statements

The School will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes for which it was collected.

Every effort will be made to ensure that data held is accurate and up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the relevant Privacy Notice and lawfully processed in accordance with the conditions for processing. (see Privacy Notices section below)

Personal Data

The School and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the School community – including students*, members of staff, and parents**, e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data, e.g. class lists, student progress records, reports, references
- Professional records, eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents or by other agencies working with families or staff members.

Responsibilities

The School's Senior Information Risk Officer (SIRO) is: Nigel Everett, Deputy Head Communication and Innovation

The SIRO will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the School's information risk policy and risk assessment
- appoint appropriate Information Asset Owners (IAOs)

The School has identified IAOs for the various types of data being held student information, staff information, assessment data etc.).

These are:

- Corinna Florence, Registrar (Student and parent information)
- Judy Wilson, Bursars' PA (Staff information)
- Alex D'Arcy Irvine, Head of Finance (Parent and financial information)
- George Budd, Academic Deputy (Assessment information)
- Niamh Green, Deputy Head Pastoral (Student pastoral information)
- Sarah Sowton, OGA (Alumni information)
- Caroline Jarrett, Financial Controller (Payroll information)
- Gill Davey, School Nurse (Medical information)
- Claire Firth, Learning Support Coordinator (Student special needs information)
- Ed Gillies, Head of ICT Services (Users' ICT information)
- Moyra Rowney, Director of External Relations (Pupil, parent, donor and related information)

The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the School has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

* The term 'student' or 'students' in this document is used to refer to pupils and students.

** The term 'parent' or 'parents' in this document is used to refer to parents and carers

Registration

The School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner (https://ico.org.uk). Our Registration Number is **Z8490246.** Our Registration Expiry Date is [25 May 2017].

Privacy Notices

In order to comply with the fair processing requirements of the DPA, the School will inform each relevant category of data subjects with which it deals of the data it collects, processes and holds, the purposes for which the data is held and the third parties to whom it may be passed. This will apply to students, parents of students, staff, donors and others as appropriate, and will be done by use of the relevant privacy notice, through the Parental Contract, the School Website (http://www.godolphin.org) or otherwise as applicable. Copies of the relevant privacy notices are available in Appendix 1.

Training & awareness

All staff will receive data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings and Inset
- Day to day support and guidance from Information Asset Owners
- Communications from the School's Online Safety Committee

Risk Assessments

Information risk assessments will be carried out by IAOs to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (see Appendix 2)

Impact Levels, use of technologies, and Protective Marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	**Impact Level (IL)**	**Applies to schools?**
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

Most student or staff personal data that is used within educational institutions will come under the PROTECT classification. However, some, eg the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer eg. "Securely delete or shred this information when you have finished using it".

The following page provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of students work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically, schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about school closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Secure Storage of and access to data

The School will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system (Schoolbase)

All users will use strong passwords which must conform to the standards of the password policy. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on School equipment (this includes computers and portable storage media) Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

If personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected),
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
- the data must be securely deleted from the device, in line with School policy once it has been transferred or its use is complete.

The School has clear policy and procedures for the automatic backing up, accessing and restoring of all data held on its systems, including off-site backups. Please refer to the relevant policy for details.

The School has clear policy and procedures for the use of 'Cloud Based Storage Systems' (for example OneDrive, Office 365, Google Apps and Google Docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act (see below). The School will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a 'third party'. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.
All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The School recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests, as detailed in the Privacy Notice. Data subjects have the right to know:

- if the data controller holds personal data about them;
- a description of that data;
- the purpose for which the data is processed;
- the sources of that data; to whom the data may be disclosed;
- and a copy of all the personal data that is held about them.

Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of School

The School recognises that personal data may be accessed by users out of School, or transferred to other agencies. In these circumstances:

- When restricted or protected personal data is required by an authorised user from outside the School's premises (for example, by a member of staff to work from home), they should ensure that wherever possible this data is accessed via the management information system (SchoolBase) or learning platform (Firefly)
- Where restricted or personal data is stored on school systems other than SchoolBase or Firefly, eg assessment spreadsheets stored on network drives, these may be accessed remotely via the school Remote Desktop application which uses a secure password protected encrypted connection

- Users may not remove or copy sensitive or restricted or protected personal data from the School or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data, or are used to access personal data must not be accessed by other users (eg family members) when out of School
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software and password protection;
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken in this event. (NB. to carry encrypted material is illegal in some countries)

Disposal of data

The School will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log is kept of all data that is disposed of based on destruction certificates (see Appendix 3)

Audit Logging/Reporting/Incident Handling

As recommended, the activities of data users, in respect of electronically held personal data, are logged and these logs are monitored by responsible individuals. A record of these logs is held by the Head of ICT Services, Mr Edward Gillies.

The audit logs are kept to provide evidence of accidental or deliberate data security breaches, including for example loss of protected data or breaches of an acceptable use policy.

The School has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a “responsible person” for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan.

Use of Cloud Services

Many schools now use cloud hosted services (OneDrive, Office 365, Google Apps and Google Docs). The School is committed to ensuring its ICT Systems are secure and that School data and systems are protected and only accessed by authorised users. Cloud Services allow convenient access to files and data from a number of different devices. If employed in a work context however, such services also introduce risks to the security, privacy, copyright and retention of School data. Before using Cloud storage, users of the School ICT environment must consider if the usage is appropriate and follow the policy guidance set out in the School’s Online Safety Policy’. In addition, users should also ensure that when using Cloud Services, they follow guidance in the following documents to ensure they limit the risk imposed on School data

- Online Safety 2(iv). Acceptable Use Policy Agreement (Staff and Volunteer)
- Online Safety 3. Technical Security Policy]
- Appendix 5: Guidance for Schools: Cloud Hosted Services, published by SWGfL

A copy of the Cloud Services permission form is available in Appendix 4

Appendix 1: Privacy Notice for School Pupils

Godolphin

Privacy Notice for School Pupils

Data Protection Act 1998: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school. We use this personal data to:

- Support our pupils' learning;
- Monitor and report on their progress;
- Provide appropriate pastoral care; and
- Assess the quality of our services.

This information will include their contact details, assessment results, attendance information attendance information, any exclusion information, where they go after they leave us, and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information. We will also request the unique learner number (ULN) which may also give us details about learning or qualifications.

We are required by law to pass some information to the Independent Schools Council (ISC) and the Department for Education (DfE). This data is of a statistical nature and does allow for the identification of an individual pupil or family.

We will not give information about our pupils to anyone outside the school without your consent unless the law and our policies allow us to.

If you require more information about how the ISC and/or DfE store and use your information, then please visit the following websites:

http://www.isc.co.uk/ and

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you would like to request a copy of the information about you that we hold and/or share, please contact Mrs Victoria Power, PA to the Head, Godolphin School, 01722 430511 or PowerV@godolphin.wilts.sch.uk.

Godolphin School is a data controller for the purposes of the Data Protection Act and has registered its use of Personal Data with the Information Commissioner's Office. Further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website under registration number Z8490246. The school Data Protection Policies are also available on the school website.

Appendix 2: Information Risk Actions Form

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Appendix 3: Disposal of Data Destruction

Document ID	Classification	Date of Destruction	Method	Authorisation

Appendix 4: Use of Cloud Services Permission Form

Godolphin

Use of Cloud Services Permission Form

The School makes use of cloud hosting services such as Microsoft Office 365 and Google Apps for Education. Google Apps for Education services: http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent' for their children to be able to use these services.

The following services are available to each pupil/student and hosted by Google as part of the School's online presence in Google Apps for Education:

Mail - an individual email account for school use managed by the School

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Drive – online storage for all types of files and media

Using these tools, pupils[/students] collaboratively create, edit and share files and websites for School related projects and communicate via email with other pupils[/students] and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of School learning experiences, and working in small groups on presentations to share with others.

Godolphin believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent Name	
Student Name	

As the parent of the above student, I agree to my child using Google Apps for Education. Yes / No

Signed	
Date	

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)

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.

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