# All Saints' CE First School
# Data Protection Policy

Created in: February 2018
Reviewed: Dec 2019
Reviewed: September 2021

# Contents



# Rationale

We need pupil, parent and employee PERSONAL data to run our schools successfully. We are trusted to look after this essential information. In order to operate effectively, we may also collect and use information relating to the people with whom we work, such as members of the public, contractors and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government.

We are committed to ensuring that PERSONAL information is properly managed and that we ensure compliance with the 2018 General Data Protection Regulations (GDPR). We are committed to making every effort to meet our obligations under the GDPR legislation and will regularly review policies and procedures to ensure that we are doing so.

We recognise that each and every employee has a responsibility to comply with the appropriate data protection laws. Our schools and their employees should do everything within their power to ensure the safety and security of any material of a PERSONAL or sensitive nature. It is the responsibility of all members of the school community to take care when handling, using or transferring PERSONAL data so 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 the school concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office (ICO) for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to PERSONAL data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

The GDPR lays down a set of rules for processing of PERSONAL data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The GDPR requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the PERSONAL data they collect is used:

- Data must be processed fairly and lawfully.
- PERSONAL data shall be obtained only for one or more specific and lawful purposes.
- PERSONAL data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- PERSONAL data shall be accurate and where necessary kept up to date.
- PERSONAL data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
- PERSONAL data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of PERSONAL data and against accidental loss or destruction of, or damage to, PERSONAL data.
- PERSONAL data shall not be transferred to a country outside the 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.

The GDPR defines “PERSONAL Data” as data which relates to a living individual who can be identified:

- from the data, or from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The GDPR further defines “Sensitive PERSONAL Data” as PERSONAL data consisting of information as to:

- the racial or ethnic origin of the data subject,
- the political opinions of the data subject,
- the data subject’s religious beliefs or other beliefs of a similar nature,
- whether the data subject is a member of a trade union,
- the physical or mental health or condition of the data subject,
- the data subject’s sexual life,
- the commission or alleged commission by the data subject of any offence, or
- any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

## Responsibilities

The Governing Board have overall responsibility for compliance with the GDPR.

The Headteacher is responsible for ensuring compliance with the GDPR and this policy within the day to day activities of the school. The headteacher is our designated Data Protection Compliancy Officer (DPCO) and is responsible for ensuring that appropriate training is provided for all staff. The DPO is Rhiannon Terry RTerry@ttlt.org.uk

Staff need to be aware of their obligations relating to any PERSONAL data they process as part of their duties. Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to prosecution. Everyone has the responsibility of handling protected or sensitive data in a safe and secure manner.

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil information, staff information, assessment data etc.). 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.

The Governing Board is required to comply fully with this policy in the event that they have access to PERSONAL data, when engaged in their role as a Representative.

The school will hold the minimum PERSONAL data necessary to enable them to perform their function and will not hold data for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All PERSONAL data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

## 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 pupils, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

## Storage of Personal Data

Personal Data will be stored using the following guidelines:

<u>Retained whilst the children remains at the school, then passed to receiving school. Retained by last receiving school until child is 25 years of age.</u>

- Pupil's Educational Record
- Safeguarding information
- SEN Information
- Records of parental permission slips (where there has been a major incident)

<u>One Year</u>

- Pupil's work (if required)

<u>Three years</u>

- Attendance Registers

<u>Current Year + 6 Years.</u>

- Examination Results

<u>Fourteen Years</u>

- Records of visits outside the classroom

## Registration

As a school we are the legal entity responsible for the processing of PERSONAL data, and so the we are the data controller subject to GDPR registration obligations.

The school is registered as a data controller on the Data Protection Register held by the Information Commissioner's Office. The register can be checked online by visiting: https://ico.org.uk/esdwebpages/search.

## Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the GDPR, our school will inform parents / carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties such as the Local Authority and Department for Education to whom it may be passed. This privacy notice will be passed to parents / carers through a specific letter. Parents / carers of new pupils to our schools will be provided with the privacy notice as part of the admissions process. Our privacy notices can be found in Appendix A.

## Information to the School Workforce – the "Privacy Notice"

In order to comply with the fair processing requirements of the GDPR, the school will inform all staff of the data it collects, processes and holds about them, the purposes for which the data is held and the third parties such as the Local Authority and Department for Education to whom it may be passed. This privacy notice will be passed to staff through a specific letter. New staff joining our school will be provided with the privacy notice as part of their contract/induction process. Our School Workforce privacy notice can also be found in Appendix A.

## Training and Awareness

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

- Induction training for new staff
- Staff meetings / briefings / training days
- Day to day support and guidance from the DPCO, IAOs, the Admin team and ICT Support staff.

## Risk Assessments

Information risk assessments will be carried out by Information Asset Owners 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 on-going process.

## Information Classification and Protective Marking

Following incidents involving loss of data, Government has revised the Protective Marking Scheme and as of 2nd April 2014 the Government Security Classifications should be used to indicate the sensitivity of data. All Saints' First School information assets will be classified into one of the following three categories:

| UNCLASSIFIED | PERSONAL-PROTECT | PERSONAL–SENSITIVE |
|---|---|---|
| Information that is published by the Trust, its schools, or made available to the public, or that is freely available. | The majority of information that is created or processed by the Trust and its schools, including that related to routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media. | A limited subset of OFFICIAL information that could have more damaging consequences (for individuals, the Trust or its schools) if it were lost, stolen or published in the media, where there is a clear and justifiable requirement to reinforce the "need to know". |

These categories are explained in more detail below.

**The classification UNCLASSIFIED**
This applies only to information that rightly belongs in the public domain. This includes:

- information that the Trust / school publishes, for example on its website;
- other information that the Trust / school makes available to its community or members of the public, even though it does not routinely publish it;
- other information the Trust / school holds that is freely available.

There is no requirement to explicitly mark information with the classification UNCLASSIFIED.

**The classification PERSONAL-PROTECT**
All routine business operations and services should be treated as PERSONAL-PROTECT. The PERSONAL-PROTECT classification covers information related to the following:

- the day to day business of the school, service delivery and public finances;
- safety, security and resilience;
- commercial interests, including information provided in confidence and intellectual property;
- individual people – PERSONAL information that must be protected under the Data Protection Act 1998, GDPR Regulations 2018 or other legislation (for example, health records).

The word PROTECT should be written in capital letters when it is being used as a term to classify information. There is no requirement to explicitly mark routine PROTECT information with its classification. However, it is acceptable to apply the label in particular circumstances if necessary.

**The classification PERSONAL–SENSITIVE**
Some information which falls within the scope of the PERSONAL classification may need a higher degree of protection than would normally be applied. This is given a stronger classification. The classification PERSONAL–SENSITIVE applies when:

- there could be more serious consequences (for individuals, the Trust or its schools) in the event that the information is lost, stolen or published in the media; and
- there is a clear and justifiable requirement to restrict access solely to those who have a business need to know the information and who are within a trusted group.

The PERSONAL–SENSITIVE classification covers the following:

- particularly sensitive information related to identifiable individuals, where inappropriate access could have damaging consequences (for example, information related to medical records, to investigations or to vulnerable individuals);
- commercially sensitive information (for example, related to contracts or financial matters);
- information that, if disclosed inappropriately, could compromise the operational effectiveness, internal stability or security of the Trust and its schools.

The PERSONAL–SENSITIVE classification also applies to all information which is due to be destroyed.

The phrase PERSONAL–SENSITIVE should be written in capital letters when it is being used as a term to classify information. Information classified as PERSONAL–SENSITIVE must be clearly and obviously marked.

**Information combined from different sources**
When information assets are gathered together from different sources, it may be the case that the individual items have different security classifications. In these cases, the overall collection of documents or files must carry the highest level of classification from the individual items. For example, if PERSONAL–SENSITIVE information is combined with UNCLASSIFIED information, the overall collection of information would adopt the classification PERSONAL–SENSITIVE and would need to be clearly marked to show that fact.

**Additional guidance**
Most pupil or staff PERSONAL data that is used within educational institutions will come under the PERSONAL classification. However some data e.g. the home address of a child at risk will be marked as PERSONAL-SENSITIVE.

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 PERSONAL or higher.

When information is acquired or created, consideration must be given to how it should be classified.

All information classified as PERSONAL–SENSITIVE must be clearly and obviously marked with its classification, and any additional descriptors (as described above) should be added if appropriate.

Consideration should be given to whether or not PERSONAL information needs to be marked with its classification. For example, if it is considered necessary to draw attention to the fact that the information would not be expected to appear in the public domain, the PERSONAL marking should be applied.

All documents (manual or digital) that are to be marked with a classification will be labelled clearly with the wording "DOCUMENT CONTROL:" in the footer accompanied by the appropriate classification, i.e. "DOCUMENT CONTROL: PERSONAL-SENSITIVE".
Below are some examples of document control classifications for typical data processed in school.

| **Typical Information** | | **Document Control** |
|---|---|---|
| School life and events | School term times, holiday, training days, the curriculum, sports events and results, extra curricular activities, displays of pupils work, lunchtime menus, extended services, parent consultation, homework and resources, school prospectus. | Most of this information will fall into the UNCLASSIFIED category. |
| Learning and achievement | Information on how parents can support their *individual* child's learning, academic achievement, assessments, attainment, progress with learning, behaviour, IEPs. | Most of this information will fall into the PERSONAL category. There may be learners whose PERSONAL data requires an PERSONAL-SENSITIVE marking, e.g. the home address of a child at risk. |
| Safeguarding | Information pertinent to child protection issues. | Most of this information will fall into the PERSONAL-SENSITIVE category, as it should only be accessed on a "need-to-know" basis. |

Information must be stored securely in order to prevent unauthorised access. Stored information should be appropriately backed up to protect it against loss.

Access to information classified as PERSONAL and PERSONAL–SENSITIVE must be limited to those authorised to view it. Access must be granted only to those who require it in order to perform their jobs. PERSONAL and PERSONAL– SENSITIVE information must always be protected against unauthorised access. This means that users must be required to supply a user name and password, or equivalent, in order to gain access to the information.

Documents must also be securely destroyed after use, e.g. shredded. Destruction markings should also be included in the footer i.e. "Securely destroy after use".

Information that is protectively marked must keep its protective marking when it is printed, copied or transferred. Protectively marked information should be printed, copied or transferred only when necessary. All protectively marked information in portable form must be protected in transit and stored securely; it must not be left unattended without protection. For advice on encryption please contact ICT support.

Below are some examples of different uses of technology and protective marking for typical data processed in school.

| **Typical Information** | | **The Technology** | **Notes on Protect Markings** |
|---|---|---|---|
| School life and events | School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services. | 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 UNCLASSIFIED category. |
| Learning and achievement | Individual pupil 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 in person or through written reports. Occasionally email, belonging to a parent may be used.<br>Data is accessed internally on school computers and at home using Remote Access. Information is used in written form for staff assessment/analysis purposes. | Most of this information will fall into the PERSONAL category. There may be occasional when pupil's PERSONAL data requires an PERSONAL-SENSITIVE marking. For example, the home address of a child at risk. In this case, the school may decide not to make a pupil record available in the normal 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. | Most of this information will fall into the PERSONAL 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 i.e. about school closures would fall into the UNCLASSIFIED category. |

## Data Gathering

All PERSONAL data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the GDPR.

Only relevant PERSONAL data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

Digital images, such as photographs from digital cameras and scanned images, especially where pupils can be identified are also covered by the GDPR.

## 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.

All users will use strong passwords which must be changed regularly. 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). This means that ALL staff MUST lock their machines if leaving them unattended, even if for brief periods of time.

All storage media (e.g. backup tapes) 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 school computers and school STAFF iPads). Private equipment (i.e. owned by staff) must not be used for the storage of any PERSONAL data.

When PERSONAL data is stored on a portable computer system:

- the data must be encrypted and password protected,
- the device must be password protected,
- the device must offer approved virus and malware checking software, and
- the data must be securely deleted from the device, once it has been transferred or its use is complete.

School iPads are encrypted when locked. All staff must ensure that staff iPads are locked when not in use to comply with the points above.

PERSONAL data must not be kept on USB sticks or other similar portable media.

USB memory sticks may be used on school systems for the reading/writing of UNCLASSIFIED data only.

Our schools have clear procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

The school has a clear policy regarding the use of “Cloud Based Storage Systems” and is aware that data held in remote and cloud storage is still required to be protected in line with the GDPR. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. For more information see “Use of Cloud Services” in this policy.

As a Data Controller, we are 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 PERSONAL material must be held in areas not visible to the public, clearly marked as PERSONAL, with clear guidance that this data is only to be viewed by authorised staff, whether on or off site.

All paper based PERSONAL-SENSITIVE material must be held in lockable storage, whether on or off site, clearly marked as DOCUMENT CONTROL: PERSONAL-SENSITIVE, with directions to shred after use.

**Subject Access Requests**

The school recognises that under Section 7 of the GDPR, data subjects have a number of rights in connection with their PERSONAL data, the main one being the right of access. Any person whose details are held by our schools is entitled, under the GDPR, to ask for a copy of all information held about them (or a child for which they are responsible).

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.
If our school receives a written request from a data subject to see any or all PERSONAL data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.

When providing the information, the school must also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

Informal requests to view or have copies or PERSONAL data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

**Data Disclosures**

PERSONAL data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

When requests to disclose PERSONAL data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

If a PERSONAL request is made for PERSONAL data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known PERSONALly, proof of identity should be requested.

Requests from parents or children for printed class lists of the names of children in particular classes should be politely refused as permission would be needed from all the data subjects contained in the list. However, lists of first names only may be given to younger classes. Staff should be mindful that this may not be possible if there are Looked After Children in the class.

PERSONAL data will not be used in newsletters, websites or other media without the consent of the data subject.

A record should be kept of any PERSONAL data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

## Data Checking

Our schools will issue regular reminders to staff and parents to ensure that PERSONAL data held is up-to-date and accurate. Any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected 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 the LA or other agencies. In these circumstances:

- Users may not remove or copy PERSONAL or PERSONAL-SENSITIVE 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.

x Users must take particular care that computers or removable devices which contain PERSONAL data must not be accessed by other users (e.g. family members) when out of school.

x When OFFICIAL or OFFICIAL-SENSITIVE PERSONAL data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access systems (i.e. the management information system).

x If secure remote access is not possible, users must only remove or copy PERSONAL or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location. x Users must protect all portable and mobile devices, including media, used to store and transmit PERSONAL information using approved encryption software.

x Particular care should be taken if data is taken or transferred to another country, particularly outside Europe and advice should be taken from the local authority/legal services in this event.

## Use of Cloud Services

When using any cloud based services, the Trust will ensure that our schools meet all of their obligations under the GDPR, ensuring full compliance with the eight Data Protection Principles. Whilst school and pupil data may be stored and controlled in the cloud by a supplier, responsibility for all areas of data protection compliance still rests with the school.

The Trust schools use the Microsoft Office 365 cloud service. This service provides email, calendars, file storage and more for both pupils and staff.

Below is a list of questions that the Trust considered the responses to when selecting our preferred cloud services provider. The answers to these questions from Microsoft can be found in Appendix A.

x Where is the data stored? x How often is the data backed up? x Does the service provider have a clear process for recovering data?

x How does the service provider protect your privacy? x Who owns the data that you store on the platform?

x Who has access to the data? x Is PERSONAL information shared with anyone else? x Does the service provider share contact details with third party advertisers? Or serve users with ads? x What steps does the service provider take to ensure that your information is secure? x How reliable is the system?

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

As of October 2014 the Department for Education (DfE) and Information Commissioners Office (ICO) created a selfcertification framework for cloud service providers. Schools are able to use the checklists 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 GDPR-compliant manner. The Microsoft response to the self-certification framework can be found in Appendix A and demonstrates that the Office 365 cloud service allows our schools to meet their obligations under the Data Protection Act.

## 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 securely destroyed.

## Related Policies

This policy should be read in conjunction with the following policies:-

Online Safety Policy

## Review

This policy will be reviewed annually, or more regularly in the light of any significant new developments or in response to changes in guidance.

## Appendix B: Microsoft Office 365 Cloud Services

The following pages contain:

Microsoft response to our cloud services questions;
Microsoft response to the self-certification framework.

## 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 (GDPR) to all customers. GDPR 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 GDPR.

## 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.