Data Protection Policy

Created: June 2018
Review date: June 2019

Approved by Trust Board: .....

Chair of Trustees signature: _____

Contents

West Stafford Multi Academy Trust

Data Protection Policy

Rationale

We need pupil, parent and employee personal data to run our Academies 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 1998 Data Protection Act (DPA). We are committed to making every effort to meet our obligations under the DPA legislation and will regularly review policies and procedures to ensure that we are doing so. West Stafford Multi Academy Trust are also committed to fulfilling our duties under the General Data Protection Regulation (GDPR).

We recognise that each and every employee has a responsibility to comply with the appropriate data protection laws. Our Academies 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 Academy 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 Academy concerned, can bring the Academy and the Trust into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office (ICO) for the Trust 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 DPA 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 DPA 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 DPA 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 DPA 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 Board of Trustees have overall responsibility for compliance with the DPA.

The CEO and Headteachers are responsible for ensuring compliance with the DPA and this policy within the day to day activities of the Trust and our Academies. The CEO is our designated Senior Information Risk Officer (SIRO) and is responsible for ensuring that appropriate training is provided for all staff.

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 Trust 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 Board of Trustees and Academy Committees 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 Trustee, Governor or Representative.

The Trust and its Academies 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 Trust, our Academies 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 Academy 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.

Registration

As a Multi Academy Trust (MAT), West Stafford Multi Academy Trust (WSMAT) is responsible for the activities of all the Academies in the MAT, even though some functions may have been delegated to the Headteacher of the Academy or Academy Committees. Ultimate responsibility lies with the MAT. Therefore, WSMAT is the legal entity responsible for the processing of personal data by the Academies within the MAT, and so WSMAT is the data controller subject to DPA registration obligations.

WSMAT 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 DPA, our Academies 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 Academies 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 Academy Workforce – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the Trust 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 Trust and its Academies will be provided with the privacy notice as part of their contract/induction process. Our Academy 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 SIRO, IAOs, the Business Leaders and ICT Support.

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 WSMAT information assets will be classified into one of the following three categories:

These categories are explained in more detail below.

The classification NOT PROTECTIVELY MARKED

This applies only to information that rightly belongs in the public domain. This includes:

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

There is no requirement to explicitly mark information with the classification NOT PROTECTIVELY MARKED.

The classification OFFICIAL

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

- the day to day business of the Trust / Academy, 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 or other legislation (for example, health records).

The word OFFICIAL 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 OFFICIAL information with its classification. However, it is acceptable to apply the label in particular circumstances if necessary.

The classification OFFICIAL–SENSITIVE

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

- there could be more serious consequences (for individuals, the Trust or its Academies) 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 OFFICIAL–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 Academies.

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

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

Further special labels for OFFICIAL–SENSITIVE information

Information in the OFFICIAL–SENSITIVE category may be further classified by one of two labels. In the Government Security Classifications document, these are called "descriptors". These descriptors indicate the need for common sense precautions to limit access to the information. The two labels are as follows:

- In the case of particularly sensitive information related to identifiable individuals, the additional descriptor 'PERSONAL' may be applied. Such information would be marked as OFFICIAL–SENSITIVE [PERSONAL].
- In the case of commercially sensitive information, the additional descriptor 'COMMERCIAL' may be applied.

Such information would be marked as OFFICIAL–SENSITIVE [COMMERCIAL].

The use of the descriptors is optional: all information classified as OFFICIAL–SENSITIVE must be labelled, but it is not mandatory to add one of the descriptors.

The descriptors should be written in capital letters and used only in conjunction with the OFFICIAL–SENSITIVE classification: they should never be used on their own or with any other classification.

NOT PROTECTIVELY MARKED	OFFICIAL	OFFICIAL-SENSITIVE
Information that is published by the Trust, its Academies, 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 Academies, 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 Academies) if it were lost, stolen or published in the media, where there is a clear and justifiable requirement to reinforce the "need to know".

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 OFFICIAL–SENSITIVE information is combined with NOT PROTECTIVELY MARKED information, the overall collection of information would adopt the classification OFFICIAL–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 OFFICIAL classification. However, some data e.g. the home address of a child at risk will be marked as OFFICIAL-SENSITIVE.

The Trust will ensure that all Academy staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as OFFICIAL or higher.

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

All information classified as OFFICIAL–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 OFFICIAL 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 OFFICIAL 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: OFFICIAL-SENSITIVE".

Below are some examples of document control classifications for typical data processed in Academy.

Typical Information		Document Control
Academy life and events	Academy term times, holiday, training days, the curriculum, sports events and results, extra-curricular activities, displays of pupil's work, lunchtime menus, extended services, parent consultation, homework and resources, Academy prospectus.	Most of this information will fall into the NOT PROTECTIVELY MARKED 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 OFFICIAL category. There may be learners whose personal data requires an OFFICIAL-

		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 OFFICIAL- 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 OFFICIAL and OFFICIAL–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. OFFICIAL and OFFICIAL– 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 to portable media. Protectively marked information should be printed, copied or transferred to portable media 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 a member of the ICT Team.

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

Typical Information		**The Technology**	**Notes on Protect Markings**
Academy life and events	Academy terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupil's work, lunchtime menus, extended services, parent consultation events.	Common practice is to use publicly accessible technology such as Academy websites or portal, emailed newsletters, subscription text services.	Most of this information will fall into the NOT PROTECTIVELY MARKED 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, Academies 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 OFFICIAL category. There may be pupils whose personal data requires an OFFICIAL-SENSITIVE marking. For example, the home address of a child at risk. In this case, the Academy may decide not to make this pupil record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, Academy 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 Academies 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 OFFICIAL category. However, since it is not practical to encrypt email or text messages to parents, Academies should not send detailed personally identifiable information. General, anonymous alerts i.e. about Academy closures would fall into the NOT PROTECTIVELY MARKED 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 DPA.

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 DPA.

Secure Storage of and Access to Data

The Trust 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 (for more details see the Trust ICT 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).

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 Academy equipment (this includes computers and portable storage media). If private equipment owned by staff is to be used for the storage of personal data then users will adhere to the Trust Bring Your Own Device Policy (BYOD).

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.

When personal data is stored on a USB memory stick or any other removable media:

- the media must be encrypted

Whilst authorised USB memory sticks may be used on Academy systems for the reading of data, data from Academy systems will only be writeable to Academy owned and encrypted USB memory sticks.

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

The Trust 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 DPA. The Trust 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 OFFICIAL and OFFICIAL-SENSITIVE material must be held in lockable storage, whether on or off site.

Subject Access Requests

The Trust 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. Any person whose details are held by one of our Academies is entitled, under the DPA, 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 one of our Academy's receive a written request from a data subject to see any or all personal data that the Academy holds about them this should be treated as a Subject Access Request and the Academy will respond within the 1 calendar month deadline. This deadline can be extended if the Subject Access Request is manifestly unfounded or excessive.

When providing the information, the Academy 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 Academy will comply with its duty to respond within the 1 calendar month 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 Academy 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 Academy 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 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.

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

Personal data will only be disclosed to Police Officers if they are able to supply a notice of a specific, legitimate need to have access to specific personal data.

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 Academies 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 Academy

The Trust recognises that personal data may be accessed by users out of Academy or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy OFFICIAL or OFFICIAL-SENSITIVE personal data from the Academy 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 must not be accessed by other users (e.g. family members) when out of Academy.
- 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).
- 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.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- 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 Academies meet all of their obligations under the DPA, ensuring full compliance with the eight Data Protection Principles. Whilst Academy 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 Academy.

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

Appendix B gives the GDPR compliance Policies for Cloud based providers.

As of October 2014 the Department for Education (DfE) and Information Commissioners Office (ICO) created a self- certification framework for cloud service providers. Academies 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 DPA-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 Academies to meet their obligations under the Data Protection Act.

Disposal of Data

The Academy 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:-

- WSMAT Online Safety Policy
- WSMAT ICT Policy
- WSMAT BYOD Policy
- WSMAT CCTV 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 A: Privacy Notices

The following pages contain:

- Privacy Notice for Pupils, Gnosall St. Lawrence C.E. Primary Academy
- Privacy Notice for Pupils, Haughton St. Giles C.E. Primary Academy
- Privacy Notice for Pupils, Woodseaves C.E. Primary Academy
- Privacy Notice for Staff

Gnosall St. Lawrence C.E. Academy
Privacy Notice – Pupils & their Families

The introduction of the GDPR (General Data Protection Regulations) in May requires us to explicitly state the nature, uses and sources of information we hold about our pupils and their families, and the reasons why we need that information. This document outlines that information and tells you your rights in terms of requesting access to the information we hold, how to appeal against any information we hold about your family. At the end of the document is a proforma for you to sign and return to school to confirm your acceptance of the information contained herein. This is produced twice, once as part of this document (without signature) and subsequently as a separate sheet to be signed and returned to school.

Who processes your information?

Gnosall St Lawrence Primary Academy is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. Mr Rees-Boughton (Office Manager) acts as a representative for the school with regard to its data controller responsibilities; he can be contacted on 01785 822391 or office@st-lawrence.staffs.sch.uk.

In some cases, your data will be outsourced to a third party processor; however, this will only be done with your consent, unless the law requires the school to share your data. Where the school outsources data to a third-party processor, the same data protection standards that Gnosall St Lawrence Primary Academy upholds are imposed on the processor.

Tracy Thorley is the Data Protection Officer. Her role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The data protection officer can be contacted on 01785 822391.

Why do we collect and use your information?

Gnosall St Lawrence Primary Academy holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- For safeguarding

Which data is collected?
The categories of pupil information that the school collects, holds and shares include the following:

- Personal information – e.g. names, pupil numbers and addresses
- Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility
- Attendance information – e.g. number of absences and absence reasons
- Assessment information – e.g. national curriculum assessment results
- Relevant medical information
- Information relating to SEND
- Behavioural information
- Photographs – these will be used to aid our records management and attendance procedures
- Safeguarding concerns/issues

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

How long is your data stored for?
Personal data relating to pupils at Gnosall St Lawrence Primary Academy and their families is stored in line with the school's GDPR Data Protection Policy.

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

Will my information be shared?
The school is required to share pupils' data with the DfE on a statutory basis, this includes the following:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- the school nurse / NHS

The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Gnosall St Lawrence Primary Academy is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NDP is maintained.

Gnosall St Lawrence Primary Academy will not share your personal information with any third parties without your consent, unless the law requires us to do so. The school routinely shares pupils' information with, where appropriate and/or necessary:

- Pupils' destinations upon leaving the school
- The LA, e.g. Admissions, Social Services etc

- The NHS
- The Police

The information that we share with these parties includes the following:

- Personal information such as address, dates of birth; contact details; parent/carer information
- Assessment information such as Key Stage outcomes
- Termly, half-yearly or annual Reports to Parents
- Behavioural issues or concerns
- Attendance data
- Safeguarding information

Parents are able to request that only their child's name, address and date of birth are passed to the LA by informing the school office in writing, via email or letter.

What are your rights?
Parents and pupils have the following rights in relation to the processing of their personal data.

You have the right to:

- Be informed about how Gnosall St Lawrence Primary Academy uses your personal data.
- Request access to the personal data that Gnosall St Lawrence Primary Academy holds.
- Request that your personal data is amended if it is inaccurate or incomplete.
- Request that your personal data is erased where there is no compelling reason for its continued processing.
- Request that the processing of your data is restricted.
- Object to your personal data being processed.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way Gnosall St Lawrence Primary Academy and/or the DfE is collecting or using your personal data, you can raise a concern with the ICO. The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

Where can you find out more information?
If you would like to find out more information about how we and/or the DfE collect, use and store your personal data, please visit Gov.uk or download our GDPR Data Protection Policy.

Declaration

I declare that I understand:

- Gnosall St Lawrence Primary Academy has a legal and legitimate interest to collect and process my personal data in order to meet statutory requirements.
- How my data is used.
- Gnosall St Lawrence Primary Academy may share my data with the DfE, and subsequently the LA.
- Gnosall St Lawrence Primary Academy will not share my data to any other third parties without my consent, unless the law requires the school to do so.
- Gnosall St Lawrence Primary Academy will always ask for explicit consent where this is required, and I must provide this consent if I agree to the data being processed.
- My data is retained in line with the school's GDPR Data Protection Policy.
- My rights to the processing of my personal data.
- Where I can find out more information about the processing of my personal data.

Declaration (to be returned to school)

Names:	Parent/Carer:	Parent/Carer:

I/we declare that I/we understand:

- Gnosall St Lawrence Primary Academy has a legal and legitimate interest to collect and process my/our personal data in order to meet statutory requirements.
- How my/our data is used.
- Gnosall St Lawrence Primary Academy may share my/our data with the DfE, and subsequently the LA.
- Gnosall St Lawrence Primary Academy will not share my data with any other third parties without my/our consent, unless the law requires the school to do so.
- Gnosall St Lawrence Primary Academy will always ask for explicit consent where this is required, and I/we must provide this consent if I/we agree to the data being processed.
- My/our data is retained in line with the school's GDPR Data Protection Policy.
- My/our rights to the processing of my/our personal data.
- Where I/we can find out more information about the processing of my/our personal data.

Signed:	Parent/Carer:	Parent/Carer:
Date:	Parent/Carer:	Parent/Carer:

Name(s) of pupil(s):	Class(es)

Haughton St. Giles C.E. Academy
Privacy Notice – Pupils & their Families

The introduction of the GDPR (General Data Protection Regulations) in May requires us to explicitly state the nature, uses and sources of information we hold about our pupils and their families, and the reasons why we need that information. This document outlines that information and tells you your rights in terms of requesting access to the information we hold, how to appeal against any information we hold about your family. At the end of the document is a proforma for you to sign and return to school to confirm your acceptance of the information contained herein. This is produced twice, once as part of this document (without signature) and subsequently as a separate sheet to be signed and returned to school.

Who processes your information?

Haughton St Giles Primary Academy is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. Mrs Sue Kelly (Office Manager) acts as a representative for the school with regard to its data controller responsibilities; she can be contacted on 01785 780511 or office@haughton.staffs.sch.uk.

In some cases, your data will be outsourced to a third party processor; however, this will only be done with your consent, unless the law requires the school to share your data. Where the school outsources data to a third-party processor, the same data protection standards that Gnosall St Lawrence Primary Academy upholds are imposed on the processor.

Tracy Thorley is the Data Protection Officer. Her role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The data protection officer can be contacted on 01785 780511.

Why do we collect and use your information?

Haughton St Giles Primary Academy holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- For safeguarding

Which data is collected?
The categories of pupil information that the school collects, holds and shares include the following:

- Personal information – e.g. names, pupil numbers and addresses
- Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility
- Attendance information – e.g. number of absences and absence reasons
- Assessment information – e.g. national curriculum assessment results
- Relevant medical information
- Information relating to SEND
- Behavioural information
- Photographs – these will be used to aid our records management and attendance procedures
- Safeguarding concerns/issues

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

How long is your data stored for?
Personal data relating to pupils at Haughton St Giles Primary Academy and their families is stored in line with the school's GDPR Data Protection Policy.

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

Will my information be shared?
The school is required to share pupils' data with the DfE on a statutory basis, this includes the following:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- the school nurse / NHS

The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Haughton St Giles Primary Academy is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NDP is maintained.

Haughton St Giles Primary Academy will not share your personal information with any third parties without your consent, unless the law requires us to do so. The school routinely shares pupils' information with, where appropriate and/or necessary:

- Pupils' destinations upon leaving the school
- The LA, e.g. Admissions, Social Services etc

- The NHS
- The Police

The information that we share with these parties includes the following:

- Personal information such as address, dates of birth; contact details; parent/carer information
- Assessment information such as Key Stage outcomes
- Termly, half-yearly or annual Reports to Parents
- Behavioural issues or concerns
- Attendance data
- Safeguarding information

Parents are able to request that only their child's name, address and date of birth are passed to the LA by informing the school office in writing, via email or letter.

What are your rights?
Parents and pupils have the following rights in relation to the processing of their personal data.

You have the right to:

- Be informed about how Haughton St Giles Primary Academy uses your personal data.
- Request access to the personal data that Haughton St Giles Primary Academy holds.
- Request that your personal data is amended if it is inaccurate or incomplete.
- Request that your personal data is erased where there is no compelling reason for its continued processing.
- Request that the processing of your data is restricted.
- Object to your personal data being processed.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way Haughton St Giles Primary Academy and/or the DfE is collecting or using your personal data, you can raise a concern with the ICO. The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

Where can you find out more information?
If you would like to find out more information about how we and/or the DfE collect, use and store your personal data, please visit Gov.uk or download our GDPR Data Protection Policy.

Declaration

I declare that I understand:

- Haughton St Giles Primary Academy has a legal and legitimate interest to collect and process my personal data in order to meet statutory requirements.
- How my data is used.
- Haughton St Giles Primary Academy may share my data with the DfE, and subsequently the LA.
- Haughton St Giles Primary Academy will not share my data to any other third parties without my consent, unless the law requires the school to do so.
- Haughton St Giles Primary Academy will always ask for explicit consent where this is required, and I must provide this consent if I agree to the data being processed.
- My data is retained in line with the school's GDPR Data Protection Policy.
- My rights to the processing of my personal data.
- Where I can find out more information about the processing of my personal data.

Declaration (to be returned to school)

Names:	Parent/Carer:	Parent/Carer:

I/we declare that I/we understand:

- Haughton St Giles Primary Academy has a legal and legitimate interest to collect and process my/our personal data in order to meet statutory requirements.
- How my/our data is used.
- Haughton St Giles Primary Academy may share my/our data with the DfE, and subsequently the LA.
- Haughton St Giles Primary Academy will not share my data with any other third parties without my/our consent, unless the law requires the school to do so.
- Haughton St Giles Primary Academy will always ask for explicit consent where this is required, and I/we must provide this consent if I/we agree to the data being processed.
- My/our data is retained in line with the school's GDPR Data Protection Policy.
- My/our rights to the processing of my/our personal data.
- Where I/we can find out more information about the processing of my/our personal data.

Signed:	Parent/Carer:	Parent/Carer:
Date:	Parent/Carer:	Parent/Carer:

Name(s) of pupil(s):	Class(es)

Woodseaves C.E. Academy
Privacy Notice – Pupils & their Families

The introduction of the GDPR (General Data Protection Regulations) in May requires us to explicitly state the nature, uses and sources of information we hold about our pupils and their families, and the reasons why we need that information. This document outlines that information and tells you your rights in terms of requesting access to the information we hold, how to appeal against any information we hold about your family. At the end of the document is a proforma for you to sign and return to school to confirm your acceptance of the information contained herein. This is produced twice, once as part of this document (without signature) and subsequently as a separate sheet to be signed and returned to school.

Who processes your information?

Woodseaves Primary Academy is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. Mrs Mandy Johnson (Bursar) acts as a representative for the school with regard to its data controller responsibilities; she can be contacted on 01785 284212 or finance@woodseaves.staffs.sch.uk.

In some cases, your data will be outsourced to a third party processor; however, this will only be done with your consent, unless the law requires the school to share your data. Where the school outsources data to a third-party processor, the same data protection standards that Gnosall St Lawrence Primary Academy upholds are imposed on the processor.

Tracy Thorley is the Data Protection Officer. Her role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. The data protection officer can be contacted on 01785 284212.

Why do we collect and use your information?

Woodseaves Primary Academy holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- For safeguarding

Which data is collected?
The categories of pupil information that the school collects, holds and shares include the following:

- Personal information – e.g. names, pupil numbers and addresses
- Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility
- Attendance information – e.g. number of absences and absence reasons
- Assessment information – e.g. national curriculum assessment results
- Relevant medical information
- Information relating to SEND
- Behavioural information
- Photographs – these will be used to aid our records management and attendance procedures
- Safeguarding concerns/issues

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

How long is your data stored for?
Personal data relating to pupils at Woodseaves Primary Academy and their families is stored in line with the school's GDPR Data Protection Policy.

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

Will my information be shared?
The school is required to share pupils' data with the DfE on a statutory basis, this includes the following:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- the school nurse / NHS

The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Woodseaves Primary Academy is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NDP is maintained.

Woodseaves Primary Academy will not share your personal information with any third parties without your consent, unless the law requires us to do so. The school routinely shares pupils' information with, where appropriate and/or necessary:

- Pupils' destinations upon leaving the school
- The LA, e.g. Admissions, Social Services etc

- The NHS
- The Police

The information that we share with these parties includes the following:

- Personal information such as address, dates of birth; contact details; parent/carer information
- Assessment information such as Key Stage outcomes
- Termly, half-yearly or annual Reports to Parents
- Behavioural issues or concerns
- Attendance data
- Safeguarding information

Parents are able to request that only their child's name, address and date of birth are passed to the LA by informing the school office in writing, via email or letter.

What are your rights?
Parents and pupils have the following rights in relation to the processing of their personal data.

You have the right to:

- Be informed about how Woodseaves Primary Academy uses your personal data.
- Request access to the personal data that Woodseaves Primary Academy holds.
- Request that your personal data is amended if it is inaccurate or incomplete.
- Request that your personal data is erased where there is no compelling reason for its continued processing.
- Request that the processing of your data is restricted.
- Object to your personal data being processed.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way Woodseaves Primary Academy and/or the DfE is collecting or using your personal data, you can raise a concern with the ICO. The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

Where can you find out more information?
If you would like to find out more information about how we and/or the DfE collect, use and store your personal data, please visit Gov.uk or download our GDPR Data Protection Policy.

Declaration

I declare that I understand:

- Woodseaves Primary Academy has a legal and legitimate interest to collect and process my personal data in order to meet statutory requirements.
- How my data is used.
- Woodseaves Primary Academy may share my data with the DfE, and subsequently the LA.
- Woodseaves Primary Academy will not share my data to any other third parties without my consent, unless the law requires the school to do so.
- Woodseaves Primary Academy will always ask for explicit consent where this is required, and I must provide this consent if I agree to the data being processed.
- My data is retained in line with the school's GDPR Data Protection Policy.
- My rights to the processing of my personal data.
- Where I can find out more information about the processing of my personal data.

Declaration (to be returned to school)

Names:	Parent/Carer:	Parent/Carer:

I/we declare that I/we understand:

- Woodseaves Primary Academy has a legal and legitimate interest to collect and process my/our personal data in order to meet statutory requirements.
- How my/our data is used.
- Woodseaves Primary Academy may share my/our data with the DfE, and subsequently the LA.
- Woodseaves Primary Academy will not share my data with any other third parties without my/our consent, unless the law requires the school to do so.
- Woodseaves Primary Academy will always ask for explicit consent where this is required, and I/we must provide this consent if I/we agree to the data being processed.
- My/our data is retained in line with the school's GDPR Data Protection Policy.
- My/our rights to the processing of my/our personal data.
- Where I/we can find out more information about the processing of my/our personal data.

Signed:	Parent/Carer:	Parent/Carer:
Date:	Parent/Carer:	Parent/Carer:

Name(s) of pupil(s):	Class(es)

Privacy Notice

The Academy workforce

The Trust is the data controller for the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to staff is to be processed.

Tracy Thornley the data protection officer. Their role is to oversee and monitor the school's data processing practices. This individual can be contacted via the Trust.

Where necessary, third parties may be responsible for processing staff members' personal information. Where this is required, the school places data protection requirements on third party processors to ensure data is processed in line staff members' privacy rights.

West Stafford Multi Academy Trust has the legal right and a legitimate interest to collect and process personal data relating to those we employ to work at our Academies and at the Trust, or those otherwise contracted to work at our Academies. We process personal data in order to meet the safeguarding requirements set out in UK employment and childcare law, including those in relation to the following:

- Academy Funding Agreement
- Academy's legal framework
- Safeguarding Vulnerable Groups Act 2006
- The Childcare (Disqualification) Regulations 2009

Staff members' personal data is also processed to assist in the running of the school, and to enable individuals to be paid.

If staff members fail to provide their personal data, there may be significant consequences. This includes, but is not limited to, the following:

- Employment checks:
    - Failure to provide the school with ample proof of a right to work in the UK will prevent employment at any Academy or at the Trust.
    - Employees found to be working illegally could face prosecution by law enforcement officers.
    - Failure to satisfy 'Safer Recruitment' requirements
- Salary requirements:
    - Failure to provide accurate tax codes and/or national insurance numbers could lead to issues of delayed payments or an employee paying too much tax.

In accordance with the above, staff members' personal data is used for the following reasons:

- Contractual requirements
- Employment checks, e.g. right to work in the UK
- Salary requirements
- Performance management
- Pecuniary interests

The personal data the school will collect from the school workforce includes the following:

- Names
- National insurance numbers
- Characteristics such as ethnic group
- Employment contracts
- Remuneration details
- Qualifications
- Absence information
- Emergency Contact information
- Medical conditions which might manifest themselves at work (eg asthmatic)

The collection of personal information will benefit both the DfE and LA by:

- Improving the management of workforce data across the sector.
- Enabling the development of a comprehensive picture of the workforce and how it is deployed.
- Informing the development of recruitment and retention policies.
- Allowing better financial modelling and planning.
- Enabling ethnicity and disability monitoring.
- Supporting the work of the school teachers' review body.

Staff members' personal data may be obtained and processed from third parties where the law requires the Trust to do so, e.g. medical records from a GP. The categories of data obtained and processed from third parties include:

Where data is obtained from third parties, the personal data may originate from sources such as:

- Doctors or other medical practitioners (eg physiotherapists)
- Health & Safety
- Occupational Health

How is your information shared?

West Stafford Multi Academy Trust will not share your personal information with any third parties without your consent, unless the law requires us to do so.

We are required, by law, to pass on some personal information to our LA and the DfE. This includes the following:

- [Outline data shared with the DfE and LA.]

How long is your data retained for?

Staff members' personal data is retained in line with each Academy's Records Management Policy.

Personal information may be retained for the following periods depending on the nature of the information. Data will only be retained for as long as is necessary to fulfil the purposes for which it was processed and will not be retained indefinitely.

If you require further information regarding retention of data, and the periods for which your personal data is held for, please download our Records Management Policy.

As the 'data subject', you have specific rights to the processing of your data.

You have a legal right to:

- Request access to the personal data that West Stafford Multi Academy Trust holds.
- Request that your personal data is amended.
- Request that your personal data is erased.
- Request that the processing of your data is restricted.

Where the processing of your data is based on your explicit consent, you have the right to withdraw this consent at any time. This will not affect any personal data that has been processed prior to withdrawing consent.

Staff members also have the right to lodge a complaint with the Information Commissioner's Office (ICO) in relation to how West Stafford Multi Academy Trust processes their personal data.

If you require further information about how we and/or the DfE store and use your personal data, please visit the Gov.UK website.

Appendix B: Cloud Services

The following pages contain:

- Microsoft response to cloud services questions
- Dropbox Data Protection Policy
- Apple Data Protection Policy

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.

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 data centers (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.

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.

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.

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.

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. Our recommendation is that schools use a Microsoft partner or support organisation with industry specific expertise in cloud services for schools.

Dropbox

Privacy and Data Protection

Introduction

Personal data plays a huge part in society and the economy. Increasingly, people seek greater control and clarity about how their personal data is used and protected by organizations they interact with. At the same time, people are looking for organizations to be given clear guidelines to protect personal data.

At Dropbox, trust is the foundation of our relationship with millions of people and businesses around the world. We value the confidence you've put in us and take the responsibility of protecting your personal data seriously.

Our Commitments to You

We're committed to protecting your personal data. Dropbox's Terms of Service outline your responsibilities when using our services. Our Privacy Policy describes our privacy commitments to users and explains how we collect, use, and handle your personal data when you use our services. If you reside in the European Union (EU), your personal data is

controlled by Dropbox International Unlimited Company based in Ireland.

If you are a Dropbox Business
or Dropbox Education user,
your organization acts as the data controller for any personal data provided to Dropbox in connection with your use of Dropbox Business or Dropbox Education. The data

controller determines the purposes and means of processing personal data. Dropbox acts as the data processor, processing data on your organization's behalf when you use Dropbox Business or Dropbox Education, and our Business Agreement includes commitments related to data processing and international data transfer.

Please note, while the scope of our certifications and audit reports typically refers to Dropbox Business and Dropbox Education, the major- ity of our controls are applicable for Dropbox Basic, Plus, and Professional users as well. More information on the standards that we comply with and how we verify our practices can be found on our compliance web page.

Our Track Record: Compliance

Compliance is an effective way to validate a service's trustworthiness. We encourage and are pleased
to provide independent verification that our security and privacy practices comply with the most widely accepted standards and regulations, such as like ISO 27001, ISO 27017, ISO 27018, Germany BSI C5, and SOC 1, 2, and 3. For

example, we were one of the first cloud service providers to achieve certification with ISO 27018, the internationally recognized standard for leading practices in cloud privacy and data protection. Our independent third-party auditors test our controls and provide their reports and opinions. We may share these with you whenever possible.

For more detail on Dropbox security features and policies, please review the Dropbox Business Security Whitepaper or contact sales@dropbox.com

Dropbox

Dropbox Architecture: Protecting

Your Personal Data

At Dropbox, we believe protecting your personal data begins with keeping your data secure. To that end, Dropbox is designed with multiple layers of protection, including secure file data transfer, encryption, and application-level controls that are distributed across a scalable, secure infrastructure.

Our Infrastructure: Files

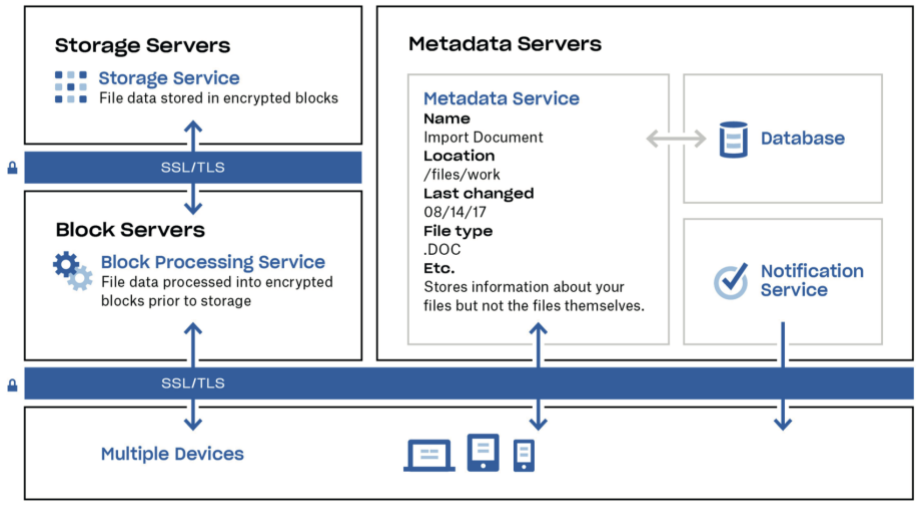
Dropbox's infrastructure for files is comprised of the components depicted in the diagram below.

Metadata Servers

Certain basic information, called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.

Storage Servers

Once files have been split into blocks and encrypted by the Block Servers, the actual contents of these file blocks are stored on the Storage Servers. The Storage Servers act as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.



Block Servers

By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. Block Servers process files from the Dropbox applications by splitting each file into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the Block Servers of the change, and new or modified file blocks are processed and transferred to the Storage Servers.

Notification Service

This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the Metadata Servers securely

to synchronize any changes.

For more detail on Dropbox security features and policies, please review the Dropbox Business Security Whitepaper or contact sales@dropbox.com

Dropbox

Our Infrastructure: Paper

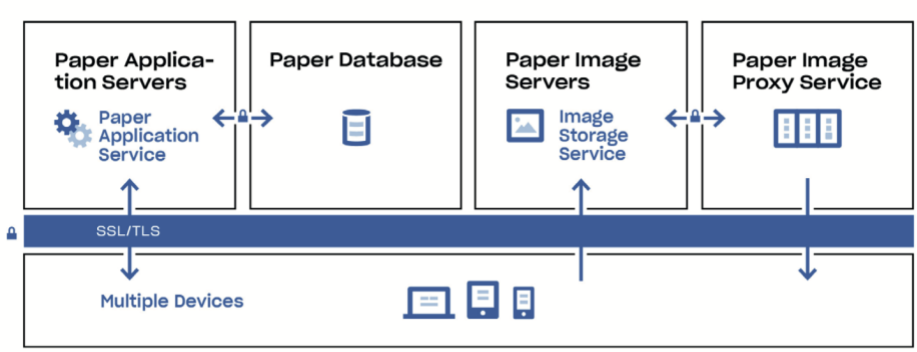
Dropbox Paper (Paper) is a feature of the Dropbox product. However, Paper uses a mostly distinct set of systems within the Dropbox infrastructure environment. Paper's infrastructure is comprised of the components depicted in the diagram below.

Paper Application Servers

The Paper Application Servers process user requests, render the output of edited Paper docs back to the user, and perform notifica- tion services. Paper Application Servers write inbound user edits to the Paper Databases, where they are placed in persistent storage. Communication sessions between the Paper Application Servers and Paper Databases are encrypted using a strong cipher.

Paper Image Servers

Images uploaded to Paper docs
are stored and encrypted at rest on the Paper Image Servers. Trans- mission of image data between the Paper Application and Paper Image Servers occurs over an encrypted session.



Paper Image Proxy Service

The Paper Image Proxy Service delivers image previews both for images uploaded to Paper docs, as well as hyperlinks embedded within Paper docs. For images uploaded
to Paper docs, the Paper Image Proxy Service fetches image data stored in the Paper Image Servers via

an encrypted channel. For hyperlinks embedded within Paper docs, the Image Proxy Service fetches image data from the source link and renders a preview of the image using either HTTP or HTTPS as specified by

the source link.

Paper Databases

The actual contents of users' Paper docs, as well as certain metadata about these Paper docs, are encrypted in persistent storage on the Paper Databases. This includes information about a Paper doc (such as the title, shared membership and permissions, project and folder associations, and other information), as well as content within the Paper doc itself, including comments and tasks. The Paper Databases are sharded and replicated as needed to meet performance |and high availability requirements.

For more detail on Dropbox security features and policies, please review the Dropbox Business Security Whitepaper or contact sales@dropbox.com

Dropbox

Dropbox Controls: Our

Internal Practices

We take comprehensive measures to protect our infrastructure, network, and applications, train employees in security and privacy practices, and build a culture where being worthy of trust is a priority. Details of some of our controls are described below:

Training

Part of protecting our users' personal data involves building and growing
a culture of security and privacy awareness. Dropbox employees are required to agree to security policies, including a user data privacy policy, prior to being granted systems access. Employees also take part in mandatory security and privacy training for new hires, as well as annual follow-up training. Employees also receive regular awareness training via informational emails, talks, presentations, and resources available on our intranet.

Encryption in Transit

To protect file data in transit between a Dropbox client (currently desktop, mobile, API, or web) and Dropbox's front-end servers, an encrypted connection is negotiated to ensure secure delivery. Similarly, an encrypted connection is negotiated to protect Paper doc data in transit between a Paper client (currently mobile, API, or web) and the hosted service. These connections are en-

crypted using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to create a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption.

Encryption at Rest

Files uploaded by users are stored on Dropbox's Storage Servers as discrete file blocks. Each block is encrypted using 256-bit Advanced Encryption Standard (AES). Only blocks that have been modified between revisions are synchronized. Similarly, Paper doc data stored on Paper Databases is also encrypted at rest using 256-bit Advanced Encryption Standard (AES).

Permanent Deletion of Files
and Paper docs
When any Dropbox user, or an administrator for a Dropbox Business or Dropbox Education team, marks a file for permanent deletion, it triggers a process to permanently delete the file. Likewise, when a user, or an administrator for a

Dropbox Business or Dropbox Education team, marks a Paper doc for permanent deletion, there is a similar process to permanently delete Paper doc data and image data.

Personal Data Access Requests

For information beyond the files
and Paper docs that are stored with Dropbox, users can sign in to the website and go to their account pages. The account page will show information like the name and email address associated with the account. Users can also view the IP addresses of connected sessions, computers, and mobile devices, as well as apps connected to their accounts from the security page and connected apps page.

Dropbox users also have the ability to request access to or the deletion of other personal information we may have collected about them. More in- formation about this process can be found in the Dropbox Help Center.

For more detail on Dropbox security features and policies, please review the Dropbox Business Security Whitepaper or contact sales@dropbox.com

Government Data
Request Principles.
We understand that when users entrust us with their personal data, they expect us to keep that data confidential. Like most online ser- vices, Dropbox sometimes receives requests from governments seeking information about its users.

The principles below describe how we handle the government data requests we receive.

Be transparent

We believe online services should be allowed to publish the number and types of government requests they receive, and to notify individuals when information about them has been requested. This type of transparency empowers users by

helping them better understand instances and patterns of govern- ment overreach. We will continue to publish detailed information about these requests and advocate for

the right to provide more of this important information.

Fight overly broad requests

Government data requests should be limited in the information they seek and narrowly tailored to spe- cific people and legitimate investi- gations. We will resist blanket and overly broad requests.

Provide trusted services

Governments should never install backdoors into online services
or compromise infrastructure to obtain user data. We will continue to work to protect our systems and

to change laws to make it clear that this type of activity is illegal.

Protect all users

Laws that give people different protections based on where they live or their citizenship are antiquated and don't reflect the global nature of online services. We will continue to advocate for the reform of these laws.

These principles, along with our annual transparency report, are made publicly available on the Dropbox website at: https://www. dropbox.com/transparency.

For additional details about our controls and our approach to protecting your personal data, please refer to our Dropbox Business Security Whitepaper.

rigorous vetting process, including security reviews and regular con- tractual reviews, to evaluate their ability to meet our data protection commitments.

strong contractual guarantees around the privacy of its services and relies on EU Model Contract Clauses to cover its international transfers of data.

Others Working for Dropbox

Dropbox manages the majority of activities related to the provision
of our services; however, we do utilize some trusted third parties in relation to our services (for example, providers of customer support and IT services). These third parties

will only access your information
to perform tasks on our behalf in compliance with our Privacy Policy, and we'll remain responsible for their handling of your information in accordance with our instructions. Each third party goes through a

International Data Transfers

Dropbox relies upon a variety
of legal mechanisms for its international transfer of personal data from the EU to the United States. We are certified under the EU-U.S. and Swiss-U.S. Privacy

Shield Programs regarding the collection, use, and retention of personal data and its transfer from the EU and Switzerland to the United States. In addition to Privacy Shield, Dropbox also provides

GDPR: The General Data Protection Regulation

The General Data Protection Regulation, or GDPR, is an EU regulation that establishes a new legal framework to protect the personal data of EU residents. The GDPR is the most significant piece of European data protection legislation since the EU Data Protection Directive of 1995, and many companies—including Dropbox—that do business in

Europe have invested heavily in GDPR compliance.

The GDPR aims to harmonize and bring data protection laws across Europe up to speed with the rapid technological change that has occurred in the past two decades.
It builds upon past legal frameworks in the EU, including the EU Data Protection Directive, and introduces

new obligations and liabilities
for organizations that handle personal data, as well as new rights for individuals in respect of their personal data. Organizations that are established in the EU, as well as organizations that process personal data of EU residents, are required to comply with the GDPR.

our systems. These exercises are sometimes referred to as performing Data Mappings and completing Data Protection Impact Assessments.

Since then, we have continued
to build on our existing internal processes and procedures to ensure we meet the accountability principles under the GDPR requirements. This is important as the GDPR places
an increased focus on documenting decisions and practices affecting personal data.

Dropbox's GDPR Compliance Journey

Dropbox is committed to GDPR compliance. Respect for privacy and security was built into our business from the beginning, and as we've grown, our focus on handling and protecting the data that our users entrust to us has remained a priority. Dropbox has a track record of staying ahead of the compliance curve — as described above, we were one of the first cloud service providers to achieve ISO 27018 certification for our business users. Given this strong foundation,Dropbox views GDPR compliance as an evolution of our existing practices and controls.

Dropbox's journey to GDPR compliance began as soon as the regulation was adopted in 2016. Our first step was to form

a cross-functional team of data protection specialists consisting
of legal counsel, security and compliance professionals, and product and infrastructure engineers. Our team then completed a full assessment of our current security and data protection practices against the GDPR requirements. Our next step was to perform an evaluation of our personal data processing activities and trace the lifecycle of personal data through

For more detail on Dropbox security features and policies, please review the Dropbox Business Security Whitepaper or contact sales@dropbox.com

Empowering our Users on

their GDPR Journeys

Dropbox provides control and visibility features that can help you manage your data protection obligations, including GDPR compliance obligations, more easily. Of course, GDPR compliance across your organization does not begin or end with the relationship with your suppliers, such as Dropbox. While our features can help you manage your obligations, they cannot ensure compliance in and of themselves. GDPR compliance requires thinking more broadly about how data moves around and is protected in your organization. Each organization should undertake its own steps to reach compliance, with suppliers as important partners on that journey.

Data Minimization

An important element of the new GDPR requirement for Privacy by Design is that organizations should design their services in a data minimizing way. This means having good visibility and control of the data within your organization in order to help you manage it. The Dropbox admin dashboard is a useful tool to help with this, as it enables you to monitor team activity, view connected devices, and audit sharing activity.

Protection and
Restoration of Data

Lost device protection, version history, and file recovery can help protect against accidental loss, damage, or destruction of personal data, and can help with the ability to restore availability and access to personal data in a timely manner in the event of an incident. Two-factor authentication is another important measure that we encourage to help protect your data.

Record Keeping

The GDPR also increases obligations on organizations to keep detailed records of their processing activities. Our audit logs and our activity logs can help your better understand your processing activities to support your record keeping.

Access Administration

Within the Dropbox admin dash- board, you easily manage team member access to files, folders, and Paper docs. For shared file links, our link permissions feature allows you to password protect the shared links, set expiration dates to grant temporary access, and limit access to those within your organization.

In the event that responsibilities change between users, our account transfer tool allows you to easily transfer files and ownership of Paper docs from one user to another. Administrators also have the ability to disable a user's access to their account while preserving their data

and sharing relationships to keep your organization's information safe. Lastly, the remote wipe feature allows you to clear files and Paper docs from lost or stolen devices.

EU Infrastructure

While the GDPR does not require personal data to be hosted within the EU in most circumstances, Dropbox does offer qualified Dropbox Business and Dropbox Education customers the ability to store files (blocks) in the EU. EU-based

file storage is provided on Amazon Web Services (AWS) infrastructure. To learn more about our EU infrastructure, contact our sales team.

For more detail on Dropbox security features and policies, please review the Dropbox Business Security Whitepaper or contact sales@dropbox.com

Dropbox

Working Together to Protect Your Personal Data

Dropbox works with its users to protect their personal data. We take comprehensive measures to protect our infrastructure, network, and applications, train employees in se- curity and privacy practices, build a culture where being worthy of trust is the highest priority, and put

Summary

our systems and practices
through rigorous third-party testing and auditing.

However, users also play a key role in protecting their personal data. Dropbox enables you to configure, use, and monitor your account in

ways that meet your organization's privacy, security, and compliance needs. Our shared responsibility guide can help you to understand more about what we do to keep your account safe and what you can do to maintain visibility and control over your personal data.

Every day, millions of users place their trust in Dropbox. To be worthy of that trust, we built and will continue to grow Dropbox with an emphasis on security and privacy. Our commitment to protecting our users' personal data is at the heart of each decision we make. For more information, please email privacy@ dropbox.com. For more information on GDPR, you can also visit our GDPR guidance center.

Apple Privacy Governance

At Apple we design our products and services according to the principle of privacy by default and collect only the minimum amount of data necessary to provide our users with a product or service. We also deploy industry-leading consent mechanisms to allow our customers to chose whether to share data such as their Location, Contacts, Reminders, Photos, Bluetooth Sharing, Microphone, Speech Recognition, Camera, Health, HomeKit, Media & Apple Music and Motion & Fitness Data with apps.

Apple has a cross-functional approach to privacy governance. Privacy governance covers all areas of the company and includes both customer and employee data. The Legal Team has a Senior Director in charge of Privacy and Law Enforcement Compliance who reports directly to Apple's General Counsel. Apple also has a Privacy Engineering Team that partners with the Privacy Legal Team and dedicated Product Counsel to design products from the ground up to protect customer privacy. Apple also has a Privacy Board made up of a cross functional group of senior representatives of Internet Software and Services, Software Engineering, Government Affairs, Product Marketing, Corporate Communications and Privacy Legal. The Privacy Board addresses privacy issues for escalation to Apple's executives. The Audit and Finance Committee of the Board of Directors assists the Board of Directors with the oversight and monitoring of privacy and data security.

All Apple employees are required to take annual training on Business Conduct. Privacy training is an essential part of Business Conduct Training. Apple requires its employees who have access to Apple customer data and personal information to undergo a Privacy Training course on a bi-annual basis. There is also additional training provided to employees who handle sensitive personal information or as required by local law.

As part of our EU General Data Protection Regulation (GDPR) work, we are undertaking Privacy Impact Assessments (PIA) of our major products and services and integrating PIAs as we develop new products and services. We also fully assess all acquisitions. These PIAs take into consideration how laws affect privacy and assess any associated privacy risks. Apple also regularly engages with a wide range of civil society representatives globally on various privacy issues including privacy by design and encryption.

Apple maintains current ISO 27001 and 27018 certifications. Apple undergoes yearly re-audits in order to receive these certifications.

Data Security and Incident Response

To make sure your personal information is secure, we strictly enforce privacy safeguards within the company. This means we use access management and access controls commensurate with the risk to data to ensure access to data is associated with a business need, such as providing you with support. Our iOS Security White Paper provides in-depth technical details as to how we have designed our products and services to protect your security including on iOS, iMessage, FaceTime, ApplePay, and iCloud. It also contains an overview of our Security Bounty Program. Information about macOS Security can be found on our macOS Security Page.

When Apple becomes aware that it may have experienced a data security incident that might impact our users' personal information, we investigate to learn what happened and determine what steps to take in response.

We analyze these facts — in the context of applicable laws, regulations, industry norms, and most of all Apple's established commitment to privacy — to determine whether we should notify affected individuals, or other relevant parties like regulators. Apple complies with all applicable laws that require notification about data security incidents.

That means we conduct prompt investigations and analysis, so that we can provide notification in a timely manner when necessary. We are also committed to providing users that have been impacted by an incident with appropriate assistance, which may include information on steps they can take to reduce the risk of harm or support from AppleCare.