St Matthew's CofE Primary School
Data Protection Policy

Policy Author:	*Roger Clarke*
Approved by/when:	*Governing Body Every 2 years*
Date of last approval:	*May 2018*
Version	*v1.01*
Due for review:	*May 2020*

TABLE OF CONTENTS

1. OVERVIEW

St Matthew's CofE School's reputation and future growth are dependent on the way the school manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the school.

As an organisation that collects, uses and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, governors, parents and visitors the School recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the School's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The School has implemented this Data Protection Policy to ensure all School Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data.

This will maintain confidence in the School and will provide for a successful working and learning environment for all.

School Personnel will receive a copy of this Policy when they join the School and may receive periodic revisions of this Policy. This Policy does not form part of any member of the School Personnel's contract of employment and the School reserves the right to change this Policy at any time. All members of School Personnel are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the School's compliance with this Policy.

2. ABOUT THIS POLICY

This Policy (and the other policies and documents referred to in it) sets out the basis on which the School will collect and use Personal Data either where the School collects it from individuals itself, or where it is provided to the School by third parties. It also sets out rules on how the School handles, uses, transfers and stores Personal Data.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. DEFINITIONS

3.1. **School** – St Matthew's CofE Primary

3.2. **School Personnel** – Any School employee, worker or contractor who accesses any of the School's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the School.
Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the School is the Controller of include employee details or information the School collects relating to students. The School will be viewed as a Controller of Personal Data if it decides what Personal Data the School is going to collect and how it will use it. A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

3.3. **Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

3.4. **Data Protection Officer –** Our Data Protection Officer is [tbc], and can be contacted at: [tbc].

3.5. **EU** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

3.6. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

3.7. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the School has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, potential employees, students, potential students, parents and visitors. Individuals also include partnerships and sole traders.

3.8. **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context. Personal Data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

3.9. **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

3.10. **Special Categories of Personal Data** – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4. SCHOOL PERSONNEL'S GENERAL OBLIGATIONS

4.1. All School Personnel must comply with this policy.

4.2. The Governing Body has overall responsibility for compliance with the DPA.

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

4.4. The Governing Body is required to comply fully with this policy in the event that they have access to Personal Data, when engaged in their role as a Governor.

4.5. The School will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil information, staff information, assessment data etc.). The IAOs will manage and address risks to the information and will understand:

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

4.6. School Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

4.7. School Personnel must not process, use, release or disclose any Personal Data:

4.7.1. outside the School; or

4.7.2. inside the school to School Personnel not authorised to access the Personal Data,

without a justified legal basis, or specific authorisation from their manager or the Data Protection Officer; this includes by phone calls, emails and social media.

4.8. School Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other School Personnel who are not authorised to see such Personal Data or by people outside the School.

5. RISK ASSESSMENTS

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

5.1.1. Recognising the risks that are present;

5.1.2. Judging the level of the risks (both the likelihood and consequences); and

5.1.3. Prioritising the risks.

Risk assessments are an on-going process.

6. INFORMATION CLASSIFICATION AND PROTECTIVE MARKING

6.1. Following incidents involving loss of data, the 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 and how it should be treated. Where the School classifies documents or information staff must adhere to the requirements of the related Protective Marking policy or procedure. All St Matthew's CofE Primary School information assets will be classified into one of the following three categories:

6.1.1. The classification: NOT PROTECTIVELY MARKED

6.1.2. The classification: OFFICIAL

6.1.3. The classification: OFFICIAL–SENSITIVE

These categories are explained in more detail in the Information Classification and Protective Marking Procedural guide.

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.

7. TRAINING AND AWARENESS

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

7.1.1. Induction training for new staff

7.1.2. Staff meetings / briefings / training days

7.1.3. Day to day support and guidance from the Business Leaders and ICT Support.

8. SECURE STORAGE OF AND ACCESS TO DATA

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

8.1.1. All users will use strong passwords which must be changed regularly (for more details see the e-Safety Policy). User passwords must never be shared.

8.1.2. 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).

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

8.1.4. Personal Data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by staff) must not be used for the storage of Personal Data.

8.1.5. When Personal Data is stored on a portable computer system:

8.1.5.1. the data must be encrypted and password protected,

8.1.5.2. the device must be password protected,

8.1.5.3. the device must offer approved virus and malware checking software, and

8.1.5.4. the data must be securely deleted from the device, once it has been transferred or its use is complete.

8.1.6. When any school/Personal Data is stored on a USB memory stick or any other removable media:

8.1.6.1. the media must be encrypted,

8.1.6.2. the memory stick must be a school-owned and encrypted memory stick

[Disciplinary action may be taken if unencrypted media/sticks are being used.]

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

The School has a clear policy regarding the use of cloud based storage systems, outlined in the Internet Usage Policy, and is aware that data held in remote and cloud storage is still required to be protected in line with the DPA. The School will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. For more information see the "Use of Cloud Services" policy.

9. DATA PROTECTION PRINCIPLES

9.1. When using Personal Data, Data Protection Laws require that the School complies with the following principles. These principles require Personal Data to be:

9.1.1. processed lawfully, fairly and in a transparent manner;

9.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

9.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

9.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

9.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and

9.1.6. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9.2. These principles are considered in more detail in the remainder of this Policy.

9.3. In addition to complying with the above requirements the School also has to demonstrate that it complies with them. The School has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the School can demonstrate its compliance.

10. LAWFUL USE OF PERSONAL DATA

Lawful purposes for processing ordinary Personal Data

These are set out in Article 6 of the GDPR and are as follows (paraphrased):

- ***the use of the Personal Data is for the purposes of the legitimate interests of the Controller;***
- ***the processing is necessary for the performance of a contract;***
- ***the processing is necessary for compliance with a legal obligation;***
- ***the processing is necessary in order to protect the vital interests of the individual or of another natural person;***
- ***the processing is necessary for the performance of a task carried out in the public interest; and***
- ***the individual who is the subject of the Personal Data has given consent for one or more specific purposes.***

Where a School is a public body, it <u>cannot</u> rely on the lawful purpose of legitimate interests where the processing is in the performance of a task carried out in the public interest or in the exercise of official authority. Instead, it needs to rely on one of the other lawful basis..

<u>Using consent to make your use of ordinary Personal Data lawful:</u>

Before relying on consent as the gateway for legitimising any processing, you should note that there are strict requirements on how it can be used (consent needs to be specific, freely given and informed). Consent can also be withdrawn at any time meaning that the Personal Data can no longer be processed.

In addition, in terms of the School's relationships with its employees, ICO guidance has stated that consent is not available in an employer and an employee relationship. The reasoning behind this is that the relationship is imbalanced and so the employee cannot really refuse to give their consent. Similarly, the ICO has commented that, for similar reasons, public authorities such as Schools will find it difficult to rely on their position of power (e.g. over students).

The School needs to ensure that for each type of ordinary Personal Data it processes it has established one of the above legal bases for processing it.

<u>Lawful purposes for Special Categories of Personal Data</u>

There are additional conditions which need to be met in order to use Special Categories of Personal Data. These are set out in Article 9 and are as follows (paraphrased):

- ***explicit consent;***
- ***employment and social security obligations;***
- ***vital interests;***
- ***necessary for establishment or defence of legal claims;***
- ***substantial public interest; and***
- ***various scientific and medical issues.***

10.1. In order to collect and/or use Personal Data lawfully the School needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing]

10.2. In addition when the School collects and/or uses special categories of Personal Data, the School has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data].

10.3. The School has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 10.1 and 10.2. If the School changes how it uses Personal Data, the School needs to update this record and may also need to notify Individuals about the change. If School Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

11. TRANSPARENT PROCESSING – PRIVACY NOTICES

11.1. Where the School collects Personal Data directly from Individuals, the School will inform them about how the School uses their Personal Data. This is in a privacy notice. The School has adopted the following privacy notices: Prospective Staff Privacy Notice, Staff Privacy notice, Parent/Carer Privacy Notice, Student Privacy Notice and Volunteer Privacy Notice.

11.2. If the School receives Personal Data about an Individual from other sources, the School will provide the Individual with a privacy notice about how the School will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

11.3. If the School changes how it uses Personal Data, the School may need to notify Individuals about the change. If School Personnel therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the School Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

12. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA

12.1. Data Protection Laws require that the School only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 11 above) and as set out in the School's record of how it uses Personal Data. The School is also required to ensure that the Personal Data the School holds is accurate and kept up to date.

12.2. All School Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

12.3. All School Personnel that obtain Personal Data from sources outside the School shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require School Personnel to independently check the Personal Data obtained.

12.4. In order to maintain the quality of Personal Data, all School Personnel that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the School must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

12.5. The School recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The School has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the School responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

13. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

13.1. Data Protection Laws require that the School does not keep Personal Data longer than is necessary for the purpose or purposes for which the School collected it.

13.2. The School has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the School, the reasons for those retention periods and how the School securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.

13.3. If School Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if School Personnel have any questions about this Policy or the School's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

14. DATA SECURITY

The School takes information security very seriously and the School has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The School has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

15. DATA BREACH

What is a Personal Data breach?

A Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing Personal Data.

Example;
Personal Data breaches can include:

- ***access by an unauthorised third party;***
- ***deliberate or accidental action (or inaction) by a controller or processor;***
- ***sending Personal Data to an incorrect recipient;***
- ***computing devices containing Personal Data being lost or stolen;***
- ***alteration of Personal Data without permission; and***
- ***loss of availability of Personal Data.***

Note: A key element of any data security arrangements should be the ability, where possible, to prevent a Data Breach and, to react to it.

This paragraph makes reference to the School's Data Breach Notification Policy and Procedure. We would strongly advise that all Schools put this policy and procedure in place as it sets out clearly how you will respond to a breach. Please refer to the accompanying template Data Breach Notification Policy.

What happens if the School is subject to a data breach?

Under the GDPR, School's will be obliged to notify the ICO in the event of a Data Breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Notification must take place within 72 hours of the School becoming aware of the breach.

You will also be obliged to notify the individuals affected by the Data Breach as soon as possible where the breach is likely to result in a high risk to their rights and freedoms, for example identity theft or fraud or where the breach may give rise to discrimination. If you are in doubt as to whether a data breach is reportable then the ICO has set up a hotline which will give guidance on this.

You will not be obliged to notify the individuals affected where:

- ***there are technological and organisational protection measures (e.g. encryption);***
- ***the Controller has taken action to eliminate the high risk; and***
- ***it would involve disproportionate effort – in this case they must be informed some other way e.g. by a notice in newspapers.***

You will still have to notify the ICO.

When do you become aware of a data breach?

You are only aware of a data breach once you have a reasonable degree of certainty that there has been a security incident and Personal Data has been compromised. This means that it is possible for you to carry out a short investigation to establish whether there is a breach and the ability to do this needs to be factored into data breach planning.

The practicalities of dealing with a data breach

In view of the short timescale for reporting the data breach, it is important, as part of GDPR compliance, to plan for a data breach and consider matters such as how a data breach may occur, what impact it may have and how it may be rectified.

Even if it is decided that a data breach is not notifiable, all data breaches must be documented on an internal data breach register and this is something which all Schools will need to put in place. It is also important in managing the risk relating to data breach that there is a culture of encouraging disclosure through an internal reporting process.

Training

All individuals who have access to Personal Data should be appropriately trained in data protection. This should be done at a level suitable for their job roles and the interaction they will have with Personal Data. Training is important to reduce the likelihood of misuse of Personal Data and the nature and frequency of the training is also taken into consideration by the ICO in considering the appropriate sanction in the event of a breach. Training should be provided to staff that is planned, timetabled and regular. Documentation should be put together which tracks who has been trained, on what and on what date.

15.1. Whilst the School takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and School Personnel must comply with the School's Data Breach Notification Policy. Please see paragraphs 15.2 and 15.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which School Personnel need to comply with in the event of Personal Data breaches.

15.2. Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

15.3. There are three main types of Personal Data breach which are as follows:

15.4. Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a School Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

15.5. Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

15.6. Integrity breach - where there is an unauthorised or accidental alteration of Personal Data.

16. APPOINTING CONTRACTORS WHO ACCESS THE SCHOOL'S PERSONAL DATA

16.1. If the School appoints a contractor who is a Processor of the School's Personal Data, Data Protection Laws require that the School only appoints them where the School has carried out sufficient due diligence and only where the School has appropriate contracts in place.

16.2. One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

16.3. Any contract where an organisation appoints a Processor must be in writing.

16.4. You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

16.5. GDPR requires the contract with a Processor to contain the following obligations as a minimum:

16.5.1. to only act on the written instructions of the Controller;

16.5.2. to not export Personal Data without the Controller's instruction;

16.5.3. to ensure staff are subject to confidentiality obligations;

16.5.4. to take appropriate security measures;

16.5.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

16.5.6. to keep the Personal Data secure and assist the Controller to do so;

16.5.7. to assist with the notification of Data Breaches and Data Protection Impact Assessments;

16.5.8. to assist with subject access/individuals rights;

16.5.9. to delete/return all Personal Data as requested at the end of the contract;

16.5.10. to submit to audits and provide information about the processing; and

16.5.11. to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

16.6. In addition the contract should set out:

16.6.1. The subject-matter and duration of the processing;

16.6.2. the nature and purpose of the processing;

16.6.3. the type of Personal Data and categories of individuals; and

16.6.4. the obligations and rights of the Controller.

17. INDIVIDUALS' RIGHTS

17.1. GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that Schools plan how they will handle these requests under GDPR.

17.2. The different types of rights of individuals are reflected in this paragraph.

17.3. **Subject Access Requests**

17.3.1. Individuals have the right under the GDPR to ask a School to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a

possible extension if it is a complex request). In addition, you will no longer be able to charge a fee for complying with the request.

17.3.2. Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

17.4 **Right of Erasure (Right to be Forgotten)**

This is a limited right for individuals to request the erasure of Personal Data concerning them where:

17.4.1 the use of the Personal Data is no longer necessary;
17.4.2 their consent is withdrawn and there is no other legal ground for the processing;
17.4.3 the individual objects to the processing and there are no overriding legitimate grounds for the processing;
17.4.4 the Personal Data has been unlawfully processed; and
17.4.5 the Personal Data has to be erased for compliance with a legal obligation.
17.4.6 In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

17.5 **Right of Data Portability**

An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

17.5.1 the processing is based on consent or on a contract; and
17.5.2 the processing is carried out by automated means
17.5.3 This right isn't the same as subject access and is intended to give individuals a subset of their data.

17.6 **The Right of Rectification and Restriction**

17.6.1 Individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

17.6.2 The School will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with the School's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which School Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

17.7 **Right to be Informed**

17.7.1 Individuals have the right to be informed about the collection and use of their Personal Data. This is a key transparency requirement under the GDPR.

17.7.2 The school must provide individuals with information including: purposes for processing their Personal Data, retention periods for that Personal Data, and who it will be shared with. This is known as 'privacy information'.

17.7.3 The school must provide privacy information to individuals at the time it collects their Personal Data.

17.7.4 The information provided must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

17.7.5 The school must regularly review, and where necessary, update the privacy information. The school must also bring any new uses of an individual's Personal Data to their attention before processing that data.

17.8 **Right to Object**

17.8.1 The GDPR gives individuals the right to object to the processing of their Personal Data in certain circumstances.

17.8.2 Individuals have an absolute right to stop their data being used for direct marketing.

17.8.3 In other cases where the right to object applies the school may be able to continue processing if it can show it has a compelling reason for doing so.

17.8.4 The school must tell individuals about their right to object.

17.8.5 An individual can make an objection verbally or in writing.

18 MARKETING AND CONSENT

18.1 The School will sometimes contact Individuals to send them marketing or to promote the School. Where the School carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

18.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR will bring about a number of important changes for organisations that market to individuals, including:

18.3 providing more detail in their privacy notices, including for example whether profiling takes place; and

18.4 rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.

18.5 Schools also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any Personal Data

18.6 Consent is central to electronic marketing. We would recommend that best practice is to provide an un-ticked opt-in box.

18.7 Alternatively, the School may be able to market using a “soft opt in” if the following conditions were met:

18.7.1 contact details have been obtained in the course of a sale (or negotiations for a sale);

18.7.2 the School are marketing its own similar services; and

18.7.3 the School gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

19 AUTOMATED DECISION MAKING AND PROFILING

19.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

Automated Decision Making happens where the School makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

Profiling happens where the School automatically uses Personal Data to evaluate certain things about an Individual.

19.2 Any Automated Decision Making or Profiling which the School carries out can only be done once the School is confident that it is complying with Data Protection Laws. If School Personnel therefore wish to carry out any Automated Decision Making or Profiling School Personnel must inform the Data Protection Officer.

19.3 School Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

19.4 The School does not carry out Automated Decision Making or Profiling in relation to its employees.

20 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

20.1 The GDPR introduce a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (“DPIA”). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

20.2 describe the collection and use of Personal Data;

20.3 assess its necessity and its proportionality in relation to the purposes;

20.4 assess the risks to the rights and freedoms of individuals; and

20.5 the measures to address the risks.

20.6 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk.

20.7 Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

20.8 Where the School is launching or proposing to adopt a new process, product or service which involves Personal Data, the School needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The School needs to carry out a DPIA at an early stage in the process so that the School can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

20.9 Situations where the School may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

20.9.1 large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

20.9.2 large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

20.9.3 systematic monitoring of public areas on a large scale e.g. CCTV cameras.

20.10 All DPIAs must be reviewed and approved by the Data Protection Officer.

21 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EU

21.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EU but also includes storage of Personal Data or access to it outside the EU. It needs to be thought about whenever the School appoints a supplier outside the EU or the School appoints a supplier with group companies outside the EU which may give access to the Personal Data to staff outside the EU.

21.2 So that the School can ensure it is compliant with Data Protection Laws School Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

21.3 School Personnel must not export any Personal Data outside the EU without the approval of the Data Protection Officer.