ST MARY'S COLLEGE DATA PROTECTION POLICY

Data Protection and GDPR

Created: August 2019 Approved: [September 2019

Our Mission

St Mary's College is a Roman Catholic College operating under the trusteeship of the Marist Fathers.

We base our philosophy on the true Christian values proclaimed in the gospel and seek to provide a challenging, high quality education whereby all members of the College community can grow as balanced individuals, morally, intellectually and spiritually.

Our Vision

To be the first choice provider of outstanding education to learners across Pennine Lancashire.

St Mary's College Data Protection Policy

St Mary's College needs to collect, store and process personal data in order to carry out its function as a college and meet the needs of its students.

Collecting data is a vital part of Safeguarding and Health & Safety for students and staff. It is needed to draw down student funding, to take payments or pay bursaries, to monitor and deliver learning activity, as well as being needed to serve many other important functions. However, we are committed to protecting the personal information it collects in line with GDPR legislation.

All of our Data Protection policies and procedures have been updated to reflect the new regulations.

If you have any questions or queries about how we use your data or if you would like further information on our policies and procedures, please send your queries to our Data Protection Officer.

TABLE OF CONTENTS:

APPENDIX:

1. OVERVIEW

The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

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. St Mary's College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The College has implemented this Data Protection Policy to ensure all College Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of the College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All members of College 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 College'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 St Mary's College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles uses, transfers and stores Personal Data.

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

3. DEFINITIONS

3.1. **College** – St Mary's College

3.2. **College Personnel** – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

3.3. **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 College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College 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.

3.4. **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.

3.5. **Data Protection Officer –** Our Data Protection Officer can be contacted by contacting the main college switchboard on: 01254 580464 or preferably, by email on: Dataofficer@stmarysblackburn.ac.uk

3.6. **EEA** – 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.

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

3.8. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College 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, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

3.9. **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.

3.10. **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.

3.11. **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. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

4.1. All College Personnel must comply with this policy.

4.2. College 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.

4.3. College Personnel must not release or disclose any Personal Data:

4.3.1. outside the College; or

4.3.2. inside the college to College Personnel not authorised to access the Personal Data,

without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

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

5. DATA PROTECTION PRINCIPLES

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

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

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

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

5.1.4. 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;

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

5.1.6. 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.

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

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

6. 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.

6.1. In order to collect and/or use Personal Data lawfully the College 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] [summarised in ANNEX A].

6.2. In addition when the College collects and/or uses Special Categories of Personal Data, the College 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-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/] [summarised in ANNEX B].

6.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify Individuals about the change. If College 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.

7. TRANSPARENT PROCESSING – PRIVACY NOTICES

7.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy notices:

7.1.1 - St Mary's College Privacy Notice - is applicable to:

- Students
- Staff
- contractors
- all other individuals dealing with the college on data protection.

The notice:

- Sets out the purposes for which we hold personal data on students and employees
- Highlights that our work may require us to give information to third parties such as professional advisers and external agencies.
- Provides that students and employees have a right of access to the personal data that we hold about them.

The privacy notice can be found on the College website and a copy is available in ANNEX C.

7.1.2 - St Mary's College Nurseries Employee Privacy Notice - is applicable to:

- employees of St Mary's College Nursery, St Mary's nursery at The Park and St Mary's Nursery at Wensley Fold Children's Centre. This includes permanent, temporary and casual employees including volunteers and apprentices

The notice:

- Sets out the purposes for which we hold personal data on employees
- Highlights that our work may require us to give information to third parties such as professional advisers and external agencies.
- Provides that employees have a right of access to the personal data that we hold about them.

The privacy notice is given to all new employees and a copy available upon request and details are provided in ANNEX D.

7.1.3 - St Mary's College Nurseries Data Protection Privacy Notice For Children and Parents - is applicable to:

- Children attending St Mary's College Nursery, St Mary's nursery at The Park and St Mary's Nursery at Wensley Fold Children's Centre. This includes children who take up free child care places and those who pay for sessions.

The notice:

- Sets out the purposes for which we hold personal data on children
- Highlights that our work may require us to give information to third parties such as professional advisers and external agencies.
- Provides that parents have a right of access to the personal data that we hold about them and their children.

The privacy notice is given to all parents of children enrolled at the nursery and a copy available upon request and details are provided in ANNEX E.

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

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

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

8.1. Data Protection Laws require that the College 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 7 above) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

8.2. All College 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.

8.3. All College Personnel that obtain Personal Data from sources outside the College 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 College Personnel to independently check the Personal Data obtained.

8.4. In order to maintain the quality of Personal Data, all College 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 College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

8.5. The College 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 College has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the College 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.

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

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

9.2. The College 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 College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.

9.3. If College 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 College Personnel have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

A copy of the College Retention Policy can be found in ANNEX F

10. DATA SECURITY

St Mary's College takes information security very seriously and has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. St Mary's College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Any queries or concerns regarding data security should be directed to Paul Holmes, IT Manager [P.Holmes@stmarysblackburn.ac.uk].

11. DATA BREACH

11.1. Whilst the College 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 College Personnel must comply with the College's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which College Personnel need to comply with in the event of Personal Data breaches.

11.2. 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.

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

11.3.1. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College 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;

11.3.2. **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

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

12. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA

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

12.2. 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.

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

12.4. 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.

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

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

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

12.5.3. to ensure staff are subject to confidentiality obligations;

12.5.4. to take appropriate security measures;

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

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

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

12.5.8. to assist with subject access/individuals rights;

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

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

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

12.6. In addition the contract should set out:

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

12.6.2. the nature and purpose of the processing;

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

12.6.4. the obligations and rights of the Controller.

13. INDIVIDUALS' RIGHTS

GDPR gives individuals more control about how 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.

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

13.2. **Subject Access Requests**

13.2.1. Individuals have the right under the GDPR to ask a College 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 from the day of receipt (with a possible extension if it is a complex request). In addition, there is no longer a fee for complying with the request.

13.2.2. 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.

13.3. **Right of Erasure (Right to be Forgotten)**

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

13.3.1.1. the use of the Personal Data is no longer necessary;

13.3.1.2. their consent is withdrawn and there is no other legal ground for the processing;

13.3.1.3. the individual objects to the processing and there are no overriding legitimate grounds for the processing;

13.3.1.4. the Personal Data has been unlawfully processed; and

13.3.1.5. the Personal Data has to be erased for compliance with a legal obligation.

13.3.2. 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.

13.4. **Right of Data Portability**

13.4.1. 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:

13.4.1.1. the processing is based on consent or on a contract; and

13.4.1.2. the processing is carried out by automated means

13.4.2. This right isn't the same as subject access and is intended to give individuals a subset of their data.

13.5. **The Right of Rectification and Restriction**

13.5.1. Finally, 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.

13.6. St Mary's College 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 College's Rights of Individuals Policy and Rights of Individuals Procedure.

14. MARKETING AND CONSENT

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

14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. In line with GDPR requirements St Mary's College takes into account changes for organisations that market to individuals, including:

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

14.2.2. 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.

14.3. St Mary's College is aware of and takes note 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. This applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data

14.4. Processes for obtaining and withdrawing consent are detailed in the Direct Marketing Statement (ANNEX G).

15. AUTOMATED DECISION MAKING AND PROFILING

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

Automated Decision Making happens where the College 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 College automatically uses Personal Data to evaluate certain things about an Individual.

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

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

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

16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

16.1. 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:

16.1.1. describe the collection and use of Personal Data;

16.1.2. assess its necessity and its proportionality in relation to the purposes;

16.1.3. assess the risks to the rights and freedoms of individuals; and

16.1.4. the measures to address the risks.

16.2. 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.

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

16.4. Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College 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.

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

16.5.1. 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;

16.5.2. 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

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

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

17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

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

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

17.3. College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

ANNEX A

ICO summary of 'lawful basis for processing data'

1.1 You must have a valid lawful basis in order to process personal data.

1.2 There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

1.3 Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

1.4 You must determine your lawful basis before you begin processing, and you should document it. We have an interactive tool to help you.

1.5 Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.

1.6 Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.

1.7 If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

1.8 If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

ANNEX B

Special category data

1.1 Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

1.2 In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

1.3 There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Act 2018 introduces additional conditions and safeguards.

You must determine your condition for processing special category data before you begin this processing under the GDPR, and you should document it.

ANNEX C

St Mary's College, Blackburn Privacy Statement

This Privacy Statement applies to the provision and services offered by St Mary's College Blackburn (including online activity).

The Privacy Statement describes how St Mary's College Blackburn collect, use and share information from or about you.

By using St Mary's College Blackburn website, you agree to these terms and conditions. Throughout this Privacy Statement "we" refers to St Mary's College Blackburn.

Your Privacy is important to us

At St Mary's College Blackburn, we fully recognise the importance of keeping our data secure.
We use established and rigorous security standards to protect personal information from unauthorised access or unlawful disclosure, accidental loss, damage, or destruction.
We use recognised industry protection measures in order to protect employee and customer information.
Personal employee and student ICT accounts are password protected.
We take reasonable precautions to ensure the data we collect and retain is accurate and limited to the information required to carry out processing for the purposes the data was provided and as outlined in this Privacy Statement.
We will only retain personal information for as long as necessary to fulfil the purpose for which it was collected and / or as required by law and / or contractual compliances.

Information we collect and how we use it

We will collect, store and process information about you if you use our website to apply for a course, job, contracting or an enquiry. We will use a similar process with regard to hard copy information provided by you for the same purposes. Information may also be stored where you voluntarily contribute content about yourself to our website, or by posting on one of our social media sites.

This information will be processed electronically and can include:
▪ Contact details including name, address, e mail and telephone number(s)
▪ Personal details including gender, age / date of birth, national insurance number
▪ Payment, invoicing and / or credit carddetails
▪ Personal preferences, enquiry details and other information provided by you via a form or our website
▪ Your image and any other personal information and content you provide voluntarily via social media
▪ Other personal information provided on surveys, feedback forms, correspondence or other online or face to face interaction Subject to applicable laws, we will collect, disclose and handle your information in order to:
▪ Process business transactions and related activities
▪ Supply and administer education, courses, goods and services
▪ Recruit employees, agency colleagues and contractors
▪ Evaluate and improve our business, services and website
▪ Send direct marketing materials to you if you have agreed for us to do so
▪ Meet legal and / or regulatory compliance requirements
▪ Protect against and help to prevent fraud, unauthorised activity and
▪ minimise risk

How we share your data

We share personal information with third parties who perform services on our behalf and to whom we are obliged to do so.

These include, but are not limited to:
▪ Those providing central services such as employee payroll
▪ Those printing and sending direct mail

▪ Those providing marketing services on our behalf
▪ Those hosting our website and application portal
▪ Funding bodies such as Education Skills Funding Agency
▪ Those providing regulatory services on behalf of St Mary's College Blackburn

These third parties are not authorised by us to use or disclose the information about you except for the purposes necessary to perform their function on our behalf or to comply with legal requirements. However, some organisations, including social media platforms, may use software and cookies and similar technologies for their own purposes, for which we do not hold responsibility. These organisations, third party internet sites and services will have separate privacy and data policies and practice independent of those of St Mary's College Blackburn.

We may also disclose information about you:
▪ If we are required to do so by law, regulation or legal process such as a court order
▪ In response to Government agencies and law enforcement authorities
▪ In order to establish, defend or exercise legal rights
▪ Where we feel disclosure is necessary or appropriate in connection to an investigation, suspected or actual illegal activity
▪ We transfer all or a proportion of our organisation or assets and only having taken steps to ensure security and confidentiality of your information

Some of the software utilised may result in personal information being held by third parties out-with the European Economic Area. In these circumstances, we are not responsible for ensuring your information is protected.

How to access the data we hold

You have the right to access, update, change or amend any personal data held by St Mary's College Blackburn. You may also opt out of us holding personal data for certain specific uses. If you wish to exercise this right, or if you wish to make an enquiry regarding how we process your personal information, contact:
GDPR Data Officer Human Resources
St Mary's College Blackburn
Shearbrow
Blackburn Lancashire
BB1 8DX
Or
Email Dataofficer@stmarysblackburn.ac.uk

ANNEX D – ST MARY'S COLLEGE NURSERY PRIVACY STATEMENT – EMPLOYEES

Data Protection Privacy Notice

For Employees

St Mary's Nurseries are part of St Mary's 6th Form College, the registered office address is St Mary's College, Shear Brow, Blackburn. BB1 8DX. The College is committed to protecting the privacy and security of your personal information.

This privacy notice describes how the Nurseries collect and use personal information about employees of the Nursery ("Employees"), (known collectively as "You" or "Your"), in accordance with the General Data Protection Regulation (GDPR).

St Mary's Nurseries are a "data controller". This means that we are responsible for deciding how we hold and use personal information about You. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to Employees. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide You with an updated copy of this notice as soon as reasonably practical.

It is important that Employees read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what Your rights are under the data protection legislation.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to You and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told You about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told You about.

6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation.

Employees:

We will collect, store, and use the following categories of personal information about Employees:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of an Employee’s continuous employment.
- Location of employment or workplace.
- Copy of driving licence (where applicable).
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Personnel files and training records including performance information, disciplinary and grievance information, and working time records.
- Information about your use of our information and communications systems.
- Records of any reportable death, injury, disease or dangerous occurrence.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about an Employee’s race or ethnicity.
- Information about an Employee’s health, including any medical condition, accident, health and sickness records, including:
    - where an Employee leaves employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
- details of any absences (other than holidays) from work including time on statutory

parental leave and sick leave; and

- where an Employee leaves employment and the reason for leaving is related to their health, information about that condition needed for pensions and permanent health insurance purposes.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

Employees:

We collect personal information about Employees through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of when an Employee works for us.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use Your personal information when the law allows us to. Most commonly, we will use Your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with You.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and Your interests and fundamental rights do not override those interests.

We may also use Your personal information in the following situations, which are likely to be rare:

1. Where we need to protect Your interests (or someone else's interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use Employee personal information

We need all the categories of information in the list above (see Employee section within the Paragraph entitled 'The Kind of Information We Hold About You') primarily to allow us to perform our contracts with Employees and to enable us to comply with legal obligations. The situations in which we will process Employee personal information are listed below.

- Making a decision about an Employee's recruitment or appointment.
- Checking an Employee is legally entitled to work in the UK. Paying an Employee and, if an Employee is an Employee or deemed Employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Providing any Employee benefits to Employees.
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider and any other provider of employee benefits.

- Administering the contract we have entered into with an Employee.
- Conducting performance and/or salary reviews, managing performance and determining performance requirements.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about an Employee's continued employment, engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving Employees, including accidents at work.
- Ascertaining an Employee's fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of an Employee's personal information.

If Employees fail to provide personal information

If Employees fail to provide certain information when requested, we may not be able to perform the respective contracts we have entered into with Employees, or we may be prevented from complying with our respective legal obligations to Employees.

Change of purpose

We will only use Your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use Your personal information for an unrelated purpose, we will notify the Employee, as is appropriate in the circumstances, and we will explain the legal basis which allows us to do so.

Please note that we may process an Employee's personal information without their respective knowledge or consent, as relevant to the circumstances, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in

the following circumstances:

1. In limited circumstances, with Employee explicit written consent.

2. Where we need to carry out our legal obligations or exercise rights in connection with Employee employment.

3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect an Employee interests (or someone else's interests) and the Employee as is appropriate is not capable of giving consent, or where the Employee has already made the information public.

The Nursery's obligations as an employer

We will use particularly sensitive personal information of Employees in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about the physical or mental health of an Employee, or their disability status, to ensure Employee health and safety in the workplace and to assess the fitness of Employees to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.
- We will use information about an Employee's race or national or ethnic origin, religious, philosophical or moral beliefs, or an Employee's sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need Employee consent?

We do not need the consent of Employees if we use special categories of personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach Employees for their written consent to allow us to process certain particularly sensitive data. If we do so, we will provide Employees with full details of the information that we would like and the reason we need it, so that Employees can carefully consider whether they wish to consent. Employees should be aware that it is not a condition of their contract with the nursery that they agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect the interests of You (or someone else's interests) and You are not capable of giving your consent, or where an Employee or a Parent, as is

relevant to the circumstances, has already made the information public.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so, which includes but is not limited to Disclosure and Barring Service ("DBS") checks. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

• To conduct a DBS check on each Employee, to record the date of the DBS check, the number of the DBS check and the name of the body conducting the DBS check.

We are allowed to use your personal information in this way to carry out our obligations. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified Employees of the decision and given the Employee as is appropriate 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with an Employee and appropriate measures are in place to safeguard the Employee's rights as is appropriate.

3. In limited circumstances, with explicit written consent from the Employee, as is appropriate, and where appropriate measures are in place to safeguard Employee rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either explicit written consent from an Employee as is appropriate, or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard an Employee rights as is relevant in the circumstances.

You will not be subject to decisions that will have a significant impact on You based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified the Employee as is appropriate in the circumstances.

DATA SHARING

We may have to share Employee data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of Your data and to treat it in accordance with the law.

Why might the Nursery share Employee personal information with third parties?

We will share Your personal information with third parties where required by law, where it is

necessary to administer the working relationship with You or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

”Third parties” includes third-party service providers (including contractors and designated agents), local authorities, regulatory bodies, and other entities within our group. The following third-party service providers process personal information about you for the following purposes:

- Local Authorities – for funding and monitoring reasons (e.g. equal opportunities and uptake of funded hours)
- Regulatory bodies – for ensuring compliance and the safety and welfare of the children
- Other Organisations - References – for ensuring compliance and the safety and welfare of the children

We will share personal data regarding your participation in any pension arrangement operated by a group company with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect Your personal information in line with our policies. We do not allow our third-party service providers to use Your personal data for their own purposes. We only permit them to process Your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share Your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share Your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share Your personal information with a regulator or to otherwise comply with the law.

DATA RETENTION

How long will you use my information for?

We will only retain Your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the manager. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of Your personal data, the purposes for which we process Your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise Your personal information so that it can no longer be associated with You, in which case we may use such information without further notice to You. Once you are no longer an Employee, we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about You is accurate and current. Please keep us informed if Your personal information changes during your working relationship with us.

Your rights in connection with personal information
Under certain circumstances, by law You have the right to:

- **Request access** to Your personal information (commonly known as a "data subject access request"). This enables You to receive a copy of the personal information we hold about You and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about You. This enables You to have any incomplete or inaccurate information we hold about You corrected.
- **Request erasure** of your personal information. This enables Employees to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove Your personal information where You have exercised Your right to object to processing (see below).
- **Object to processing** of Your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about Your particular situation which makes You want to object to processing on this ground. You also have the right to object where we are processing Your personal information for direct marketing purposes.
- **Request the restriction of processing** of Your personal information. This enables Employees to ask us to suspend the processing of personal information about You for example if You want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of Your personal information to another party.

If You want to review, verify, correct or request erasure of Your personal information, object to the processing of Your personal data, or request that we transfer a copy of Your personal information to another party, please contact the manager in writing.

No fee usually required

You will not have to pay a fee to access Your personal information (or to exercise any of the other rights).

What we may need from You

We may need to request specific information from You to help us confirm your identity and ensure Your right to access the information (or to exercise any of Your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where You may have provided Your consent to the collection, processing and transfer of Your personal information for a specific purpose, You have the right to withdraw Your consent for that specific processing at any time. To withdraw Your consent, please contact Tracy Ellett. Once we have received notification that You have withdrawn Your consent, we will no longer process Your information for the purpose or purposes You originally agreed to, unless we have another legitimate basis for doing so in law.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide You with a new privacy notice when we make any substantial updates. We may also notify You in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact Tracy Ellett, Nursery Area Manager.

I,_____ (Employee), acknowledge that on _____ (date), I received a copy of the Nursery's privacy notice for Employees and that I have read and understood it.

Signature

……

Name

……

ANNEX E – ST MARY'S COLLEGE NURSERY PRIVACY STATEMENT – PARENTS AND CHILDREN

Data Protection Privacy Notice

For Children and Parents

St Mary's Nurseries are part of St Mary's 6th Form College, the registered office address is St Mary's College, Shear Brow, Blackburn. BB1 8DX. The College is committed to protecting the privacy and security of your personal information.

This privacy notice describes how the Nurseries collect and use personal information about children attending the Nurseries ("Child" or "Children") and the parents of the Children ("Parents") (known collectively as "You" or "Your"), in accordance with the General Data Protection Regulation (GDPR).

St Mary's Nurseries are a "data controller". This means that we are responsible for deciding how we hold and use personal information about You. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to Children and Parents. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide You with an updated copy of this notice as soon as reasonably practical.

It is important that Children and Parents read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what Your rights are under the data protection legislation.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to You and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told You about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told You about.

6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation.

Children:

We will collect, store, and use the following categories of personal information about Children:

- Name
- Date of birth
- Home address
- Dietary requirements
- Attendance information
- Photographs and video clips of the Child to signpost Children to where their belongings are stored at the Nursery that they attend, and also for general display purposes
- Emergency contact should Parents be unavailable and the emergency contact’s contact details
- Learning Journey for each Child containing the work of the Child whilst at the Nursery, observations about the Child’s development whilst at the Nursery from Employees of the Nursery, specific examples of the Child’s progress, photographs demonstrating the Child’s development whilst at the Nursery, and personal details of the Child (e.g. their date of birth) (“Progress Report”)
- Records relating to individual Children e.g. care plans, child and family plans (CAFs), speech and language referral forms
- Accidents and pre-existing injuries forms
- Records of any reportable death, injury, disease or dangerous occurrence
- Observation, planning and assessment records of Children

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about a Child’s race or ethnicity, spoken language and nationality.
- Information about a Child’s health, including any medical condition, health and sickness records.
- Information about a Child’s accident or incident reports including reports of pre-existing injuries.
- Information about a Child’s incident forms / child protection referral forms / child protection case details / reports.

Parents:

We will collect, store, and use the following categories of personal information about Parents:

- Name

- Home address
- Telephone numbers, and personal email addresses.
- National Insurance number.
- Bank account details.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about a Parent’s race or ethnicity, spoken language and nationality.
- Conversations with Parents where Employees of the Nursery deem it relevant to the prevention of radicalisation or other aspects of the governments Prevent strategy.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

Children and Parents:

We collect personal information about Children and Parents from when the initial enquiry is made by the Parents, through the enrolment process and until the Children stop using the Nursery’s services.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use Your personal information when the law allows us to. Most commonly, we will use Your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with You.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and Your interests and fundamental rights do not override those interests.

We may also use Your personal information in the following situations, which are likely to be rare:

1. Where we need to protect Your interests (or someone else’s interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which the Nursery will use personal information of Children

We need all the categories of information in the list above (see Children section within the Paragraph entitled ‘The Kind of Information We Hold About You’) primarily to allow us to perform our obligations (including our legal obligations to Children. The situations in which we will process personal information of Children are listed below.

- Upon consent from the Parents, Personal Data of Children will be shared with schools for progression into the next stage of their education.
- Personal information of Children will be shared with local authorities without the consent of Parents where there is a situation where child protection is necessary.
- The personal information of Children will be shared with local authorities without the

consent of Parents for funding purposes.

Ofsted will be allowed access to the Nursery's systems to review child protection records.

- To ensure we meet the needs of the Children
- To enable the appropriate funding to be received
- Report on a Child's progress whilst with the Nursery
- To check safeguarding records
- To check complaint records
- To check attendance patterns are recorded
- When a Child's Progress Report is given to its Parent in order for that Parent to pass the same Progress Report to a school for application or enrolment purposes

Situations in which the Nursery will use personal information of Parents

We need all the categories of information in the list above (see Parents section within the Paragraph entitled 'The Kind of Information we Hold About You') primarily to allow us to perform our contracts with Parents and to enable us to comply with legal obligations. The situations in which we will process personal information of Parents are listed below.

- The personal information of Parents will be shared with local authorities without the consent of Parents for funding purposes.
- To report on a Child's attendance
- To be able to contact a Parent or a Child's emergency contact about their Child
- To ensure nursery fees are paid

If Parents fail to provide personal information

If Parents fail to provide certain information when requested, we may not be able to perform the respective contracts we have entered into with Parents, or we may be prevented from complying with our respective legal obligations to Children and Parents.

Change of purpose

We will only use Your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use Your personal information for an unrelated purpose, we will notify the Child or Parent, as is appropriate in the circumstances, and we will explain the legal basis which allows us to do so.

Please note that we may process a Child's or a Parent's personal information without their respective knowledge or consent, as relevant to the circumstances, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in

the following circumstances:

1. In limited circumstances, with Parent explicit written consent.

2. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect a Child or a Parents' interests (or someone else's interests) and the Child or Parent as is appropriate is not capable of giving consent, or where the or Parent has already made the information public.

AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified Parents of the decision and given the Parent 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with a Parent and appropriate measures are in place to safeguard the Child's or the Parent's rights as is appropriate.

3. In limited circumstances, with explicit written consent from the Parent, as is appropriate, and where appropriate measures are in place to safeguard Parent rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either explicit written consent from a Parent as is appropriate, or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard a Parents rights as is relevant in the circumstances.

You will not be subject to decisions that will have a significant impact on You based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified the Parent as is appropriate in the circumstances.

DATA SHARING

We may have to share Child or Parent data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of Your data and to treat it in accordance with the law.

Why might the Nursery share Child or Parent personal information with third parties?

We will share Your personal information with third parties where required by law, where it is necessary to administer the working relationship with You or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents), local authorities, regulatory bodies, schools and other entities within our group. The following third-party service providers process personal information about you for the following

purposes:

- Local Authorities – for funding and monitoring reasons (e.g. equal opportunities and uptake of funded hours)

- Regulatory bodies – for ensuring compliance and the safety and welfare of the children

- Schools – to provide a successful transition by ensuring information about the child's progress and current level of development and interests are shared

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect Your personal information in line with our policies. We do not allow our third-party service providers to use Your personal data for their own purposes. We only permit them to process Your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share Your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share Your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share Your personal information with a regulator or to otherwise comply with the law.

DATA RETENTION

How long will you use my information for?

We will only retain Your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the manager. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of Your personal data, the purposes for which we process Your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.
In some circumstances we may anonymise Your personal information so that it can no longer be associated with You, in which case we may use such information without further notice to You. Once your Child is no longer benefiting from the Nursery's services or a Parent, as is appropriate, we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about You is accurate and current. Please keep us informed if Your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law You have the right to:

- **Request access** to Your personal information (commonly known as a "data subject access request"). This enables You to receive a copy of the personal information we hold about You and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about You. This enables You to have any incomplete or inaccurate information we hold about You corrected.
- **Request erasure** of your personal information. This enables Parents to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove Your personal information where You have exercised Your right to object to processing (see below).
- **Object to processing** of Your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about Your particular situation which makes You want to object to processing on this ground. You also have the right to object where we are processing Your personal information for direct marketing purposes.
- **Request the restriction of processing** of Your personal information. This enables Parents, as is appropriate, to ask us to suspend the processing of personal information about You for example if You want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of Your personal information to another party.

If You want to review, verify, correct or request erasure of Your personal information, object to the processing of Your personal data, or request that we transfer a copy of Your personal information to another party, please contact the manager in writing.

No fee usually required

You will not have to pay a fee to access Your personal information (or to exercise any of the other rights).

What we may need from You

We may need to request specific information from You to help us confirm your identity and ensure Your right to access the information (or to exercise any of Your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where You may have provided Your consent to the collection, processing and transfer of Your personal information for a specific purpose, You have the right to withdraw Your consent for that specific processing at any time. To withdraw Your consent, please contact Tracy Ellett. Once we have received notification that You have withdrawn Your consent, we will no longer process Your information for the purpose or purposes You originally agreed to, unless we have another legitimate basis for doing so in law.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide You with a new privacy notice when we make any substantial updates. We may also notify You in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact Tracy Ellett, Nursery Area Manager.

I,_____ (Parent), acknowledge that on _____ (date), I received a copy of the Nursery's privacy notice for Children and Parents and that I have read and understood it.

Signature

……

Name

……

ANNEX F – Storage and Retention Policy - College

Data Retention Schedule - Summary

1. Purpose of this document

A vital part of the College's Data Protection Policy and practice is that personal data is retained for the appropriate period of time – neither too long nor too short. The Data Protection Policy states that it is the College's policy to:

> retain all information only for as long as specified in the Data Retention Schedule and, in general, no longer than two years plus the current year

This document is a summary of the Data Retention Schedule, and gives an indication of the kind of personal data which needs to be retained for longer than the maximum two years stipulated in the Policy.

N.B. While this document summarises and clarifies the Data Retention Schedule, running to 113 pages, it does not supersede it. The timelimits for those items subject to legislation as specified in detail in the Data Retention Schedule (and outlined in Section 3 below) remain in force, and should be referred to in cases of doubt.

2. Current plus two-year rule

As stated in the Data Protection Policy, personal data should not be held for more than two years after it ceases to be current, unless there is a specific reason for doing so (see Section 3 for the specific categories requiring different retention periods). The definition of current will vary according to the personal data: for example, it will mean until the course has finished where it relates to students, or until a member of staff has ceased being employed by the College where it relates to staff.

It should be remembered that the 'current plus two years' rule is a maximum period for retention. If there is no need to keep the personal data that long, then it should be disposed of securely before the two years time-limit.

3. Exceptions to the two-year rule

This section gives a guide to the categories which have legislation determining the length of time for which personal data within that category should be retained. An indication is given to the main section of the Data Retention Schedule dealing with this category.

Category	**Examples & Retention period**
Student records	• Enrolment forms, transfers, withdrawals, disciplinary, appeals • Bursary Records • Exams data ***Current year plus six***
Financial records	• Purchase ledger, sales ledger, cash book payments etc. • Payroll data ***Current year plus six***
Complaints	• Correspondence with complainants

		Current year plus 6
Contractual arrangements	• Service level agreements • Legal contracts • Tender documentation	
		Life of contract plus six years
Governors papers	• Articles and Instruments • Agendas and minutes of meetings	
		Current year plus six
Data Protection/FOI requests	• Correspondence regarding DP/FOIA requests	
		Current year plus six
Personnel records Personnel Data Retention Schedule	• Wide variety of specific retention limits – please see separate	
		from six months to 75 years
Health and Safety records	• Please refer to Health and Safety Officer	
		Retention Schedule Up to 50 years

ANNEX G – Using Personal Data for Direct Marketing

Under the Data Protection Act 1998 (Section 11) an individual has the express right to object to the use of their Personal Data for direct marketing purposes. 'Direct Marketing' is defined in the Act as meaning the communication of any advertising or marketing material that is directed to particular individuals.

It is obviously best practice for the direct marketer to inform the Data Subject of this right, and the Information Commissioner expects this. For this reason there are 'opt-out' boxes on Application and Enrolment forms as filled in by students allowing them to indicate their desire to exercise this right.

If we are Direct Marketing to an individual who has exercised this right we are in breach of the Act.

Any information we retain for the purpose of Direct Marketing will be retained solely for marketing and promotion of the College and shall not be passed to any third parties without first gaining the express consent of that individual.

If an individual has exercised this right, the only marketing material we could send them would be in response to a specific request. For example a student has ticked the 'opt-out' box on their enrolment form, and subsequently requests a part-time prospectus. In this case we could send a part-time prospectus, but no other material.

Data collection forms where the data collected may be used for Direct Marketing must clearly state this. They must also inform the Data Subject of their right to prevent processing for Direct Marketing purposes. For example by including a phrase such as

"We may wish to send you promotional/advertising material about our other courses/services. If you would prefer us not to do this please tick this box "

In addition, any Direct Marketing that does take place must include a note stating that the marketing is from St Marys College and that individuals have a right to prevent processing for Direct Marketing purposes. All marketing must also have a simple mechanism which allows the recipient to opt-out of receiving further marketing if they so wish, for example, a return email address.

The College will comply with any request to stop processing for Direct Marketing purposes within a reasonable period of time and in any event before the end of 28 days from the date of request.

Obviously, in order to fulfil our obligations to Data Subjects we must maintain up-to-date databases that allow us to remove or otherwise exclude individuals who have exercised their right to prevent processing. The UNIT-e database of student data is maintained as the most accurate record of students' wishes in this regard.