St Mary's Catholic School

GDPR/DPA 2018- Data Protection Policy

Contents

Introduction

The following documents are used by the school to demonstrate compliance regarding the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA2018).

The data protection officer for the school is Bryan Chapman of Chapman Data & Information Services LTD.

Privacy Notice (How we use pupil information)

The categories of pupil information that we collect, hold and/or share include:

- Personal information (such as name, unique pupil number and address, adult emergency contact information)
- Characteristics (such as free school meal eligibility, Pupil Premium Information)
- Special Categories (such as Ethnicity, Language, Nationality, Country of birth & Religion)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information (Special Category Data)
- Special Educational Needs information
- Exclusions and Behavioural information.
- Financial Information (such as dinner money transactions, trip transactions)
- Post 16 Information (such as destination data, UCAS applications and grants)

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- Financial audits
- to provide a rewards structure
- to track how well the school is performing as a whole

The lawful basis on which we use this information

We collect and use pupil information under the Education Act 1996/ Data Protection Act 1998 and EU General Data Protection Regulation **(**GDPR**)** Article 6, and Article 9 -from 25 May 2018.

Special category data from article 9 is processed under condition (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purpose, except where Union of Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. This will be via the pupil information sheet that you are requested to complete upon your child's entry to the school.

Storing pupil data

We hold pupil data if it is lawful for us to do. Any data that we are no longer required to hold lawfully is deleted/destroyed in accordance with the school's data retention guidelines

Who we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- Medical information as appropriate/necessary with the NHS
- Third party companies/partners who are assisting the school. All third-party companies/partners who process data on our behalf will have a data processing agreement with the school.

Why we share pupil information

- We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

- We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

- We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

- We share data with schools that your child attends after leaving us to assist with the school transition process.

- We share data with third party companies/partners who may require this information to assist the school.

- We share pupil data with the NHS when appropriate to assist with medical needs of children within the school.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the school. Please see the schools subject access request policy for further information.

You also have the right to:

· object to processing of personal data that is likely to cause, or is causing, damage or distress
· prevent processing for the purpose of direct marketing
· object to decisions being taken by automated means
· in certain circumstances, have inaccurate personal data rectified, restrict processing, erased or destroyed

· Data portability
· claim compensation for damages caused by a breach of the Data Protection regulations; and
· Withdraw consent for special categories by requesting a new pupil information sheet

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office: · Report a concern online at https://ico.org.uk/concerns/

· Call 0303 123 1113

· Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you would like to discuss anything in this privacy notice, please contact the data protection officer by e-mail (below) or contact the school who will pass your details to the data protection officer.

Bryan Chapman
Chapman Data and Information Services Ltd
dpo@chapmandis.co.uk

Privacy Notice (How we use School Workforce Information)

We process personal data relating to those we employ to work at, or otherwise engage to work at, our Trust. This is for employment purposes to assist in the running of the Trust and to enable individuals to be paid. The collection of this information will benefit both national and local users. For the purpose of this Privacy Notice, the term 'staff' will also apply to Trustees, Members and governors

The categories of workforce information that we collect, hold and/or share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information (such as gender, age, ethnic group)
- contract information (such as start dates, hours worked, post, roles, payroll and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- contact information (such as telephone numbers of contacts that an employee would want the Trust to contact in an emergency);
- Performance management data (such as appraisal/observation records)
- Medical information
- Addresses

Why we collect and use this information

We use the school workforce information to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Provide access to third party solutions to dispense your professional duties
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

The lawful basis on which we use this information

We process this information under the Education Act 1996 (departmental censuses), Data Protection Act 1998 and EU General Data Protection Regulation (GDPR) Article 6, and Article 9 - from 25 May 2018

Special category data from article 9 is processed under condition (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purpose, except where Union of Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

Collecting your information

Whilst the majority of the information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this. This will be via an employee information sheet.

Storing this information

We hold school workforce data if it is lawful for us to do. Any data that we are no longer required to hold lawfully is deleted/destroyed in accordance with the school's data retention guidelines.

We routinely share workforce information with:

- our local authority
- the Department for Education (DfE)
- Third party companies/partners who are assisting the school. All third-party companies/partners who process data on our behalf will have a data processing agreement with the school.

Why we share workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, staff have the right to request access to information about them that we hold. To make a request for your personal information, contact the school. Please see the schools subject access request policy for further information.

You also have the right to:

· object to processing of personal data that is likely to cause, or is causing, damage or distress
· prevent processing for the purpose of direct marketing
· object to decisions being taken by automated means
· in certain circumstances, have inaccurate personal data rectified, restrict processing, erased or destroyed
· Data portability
· claim compensation for damages caused by a breach of the Data Protection regulations; and
· Withdraw consent for special categories by requesting a new pupil information sheet

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office: · Report a concern online at https://ico.org.uk/concerns/

· Call 0303 123 1113

· Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you would like to discuss anything in this privacy notice, please contact the data protection officer by e-mail (below) or contact the school who will pass your details to the data protection officer.

Bryan Chapman
Chapman Data and Information Services Ltd
dpo@chapmandis.co.uk

Data Breach Policy

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include 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.

It is a security incident that has affected the confidentiality, integrity or availability of personal data. Whenever a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, promptly take steps to address it, including informing the ICO if required.

The ICO must be informed if the breach has resulted in a risk to people's rights and freedoms; if this is unlikely then it does not have to be reported. However, if the breach has not been reported then the school should be able to justify this decision.

In assessing if a data breach has created a risk to people's rights and freedoms then Recital 85 of the GDPR should be consulted.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

There are several courses of action that can be followed following a data breach. Advice may be given to the individual staff member specifically and/or to school staff in general. This may also result in additional training for an individual, team or whole staff. In the most serious cases and/or when there is evidence to suggest disregard for procedures then this could result in staff receiving a verbal warning, a written warning or potentially dismissal

Data Breach Process

1. Data Breach reported to either head teacher or school data protection officer. Whichever is informed, they will inform the other with immediate effect.

2. Immediate action taken to contain the breach.

3. Begin completion of the data breach document log by Data Protection Officer.

4. Any actions from data breach document log carried out.

5. Chair of Governors to be informed in a timely manner.

6. Completed data breach document log agreed by both Head Teacher and Data Protection Officer and copies kept by both.

Staff Data Processing Agreement

For the use of this document data is defined as Personal Identifiable Information (PII) or confidential information.

I agree to;

1. Never disclose or share any data to anyone who should not have access.
2. Never openly discuss data in an environment where it may be possible that a third party could overhear.
3. Destroy/delete any data that I have no lawful reason for holding.
4. Shred any paper documents that I no longer require that contains data.
5. Never willingly access data that I have no right to access.
6. Never willingly alter data without permission.
7. Never save data on a laptop/desktop that others may have access to and will always save data in the agreed locations on the network within the school.
8. Use memory sticks in accordance with the school policy.
9. Lock my computer when I leave my workstation.
10. Log out of all systems when not in use.
11. Never send data in an e-mail unless it is secure.
12. Report any concerns around data to either the school leadership or the data protection officer for the school.
13. Report any personal data breaches in accordance with the school's data breach policy.
14. Never leave data on my desk while not in attendance (clear desk policy)
15. Never share passwords.
16. Never log into a system using another person's log in.
17. Never print data unless necessary.
18. Adhere to the laws governing The General Data Protection Regulation (GDPR).

Failure to comply with the above, could lead to a data breach investigation in accordance with the school's data breach policy, which has been given to you with this document.

Signature_____

Print Name_____

Date_____

Data Protection by Design and Default Policy

Under the General Data Protection Regulation (GDPR), the school has a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Privacy by design should be a key consideration in the early stages of any project and should continue throughout its lifecycle. This allows schools to minimise privacy risks and builds trust. By designing projects, processes, products and systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage.
- Increased awareness of privacy and data protection across the school.
- The school are more likely to meet their legal obligations and less likely to breach GDPR.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

There are 7 foundational principles of privacy by design

- Proactive not reactive
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – Positive-sum, no zero-sum
- End-to-End security – Full lifecycle protection
- Visibility and transparency
- Respect for user privacy

1. **Proactive not reactive**

The Privacy by design approach is characterised by being proactive rather than reactive. By using this approach, the school will anticipate and prevent privacy invasive events before they happen. This approach means that the school are not waiting for a privacy risk to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short privacy by design comes before the fact, not after.

2. **Privacy as the default setting**

Privacy by design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy.

3. **Privacy embedded into design.**

Privacy by design is embedded into the design of school practices. It should not be a bolted add on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy becomes integral to school practices.

4. **Full Functionality – Positive-Sum, not Zero-Sum**

Privacy by design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are

made. Privacy by design avoids the pretence of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.

5. **End-to-End security – Full lifecycle protection**

Privacy by design, having been embedded into the project prior to anything else extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, privacy by design ensures cradle to grave, secure lifecycle management of information, end-to end

6. **Visibility and transparency**

Privacy by design seeks to assure everyone that whatever the practice of the school regarding personal data that it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. **Respect for user privacy**

Above all, privacy by design requires the school the protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Privacy Impact Assessment (PIAs) Policy

Privacy Impact Assessments (PIA's) are an integral part of taking a privacy by design approach. PIA's are a tool that the school can use to identify and reduce the privacy risks of a project. A PIA can reduce the risk of harm to individuals through misuse of their personal information. It can also help the school design a more efficient and effective process for handling personal data.

You can integrate the core principals of the PIA process with your existing project and risk management policies. This will reduce the resources necessary to conduct the assessment and spreads awareness of privacy throughout the school.

An effective PIA will allow the school to identify and fix problems at an early stage and PIA's are an integral part of privacy by design. PIAs are often applied to new projects. However, a PIA can also be used if the school are planning changes to an existing process.

The school have a process and guidance on how they will approach PIAs.

Privacy Risk

PIA's should assist the school in identifying privacy risk, which is the risk of harm through an intrusion into privacy. This is the risk of harm through use or misuse of personal information. Some ways that this risk can arise are through personal information being:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely.

The outcome of a PIA should be to minimise privacy risk. The school should develop an understanding of how it will approach the broad topics of privacy and privacy risk.

Benefits

The benefits of a PIA are that allows individuals to be reassured that the school which uses their information have followed best practice. A project which has been subject to a PIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way. A PIA should also improve transparency and make it easier for an individual to understand why their information is being used.
The school should also benefit from using PIA's. The process of conducting the assessment will improve how the school use information which impacts on individual privacy. This should in turn reduce the likelihood that the school will fail to meet its legal obligations.
Conducting and publishing a PIA will help the school build trust with the people using their services. The actions taken during and after the PIA process can improve the schools understanding of its stakeholders.
Consistent use of PIA's will increase the awareness of privacy and data protection within the school and ensure that all staff involved in designing projects think about privacy at the early stages.

When should we use PIAs?

The core principals of PIA can be applied to any project that involves the use of personal data, or any other activity which could have an impact on the privacy of individuals.
A PIA should be used on new projects or when making an amendment to a current project. The PIA should be built into the project management structure.

Who should carry out the PIA?

It is the school decision who is best placed to carry out the PIA. The Data Protection Officer (DPO) is well placed to have a significant role in a PIA. However, the PIA is designed to be used by anyone within the school. For the PIA to be effective it should include some involvement from various people within the school, who will each be able to identify different privacy risks and solutions.

What should the PIA do?

The PIA should be flexible so that it can be integrated with the schools existing approach to managing projects. The PIA should incorporate the following:

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process.

PIA Document Log

Screening questions to assess if a PIA is required

If the answer is yes to any of the questions below, then using a PIA may be useful.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to this information?
- Are you using the information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve using new technology which might be perceived as being privacy intrusive?
- Will the project result in the school making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, use of special category data within GDPR.
- Will the project require you to contact individuals in ways which they may find intrusive?

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Data Flow

- How is the information collected?
- How is the information stored?
- How is the information used?
- How is the information deleted?

Step two: Describe the information flows

The collection, use and deletion of personal data should be described here, and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Privacy Risks

- Are there any privacy risks to individuals?
- Are there any compliance risks to the school, such as fines for non-compliance?
- Are there any school level risks?

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.
Consultation can be used at any stage of the PIA process.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Privacy Issue	Risk to individuals	Compliance Risk	Associated organisation/corporate risk

Step four: Identify privacy solutions

Describe the actions you take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution	Result – Risk has been eliminated/reduced, or accepted	Evaluation – Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Consent Process

Sought

- For new pupils a consent form should be given to parents/carers before the child begins at the school.
- The school adopts a positive opt in approach to its consent. This means that should a parent/carer not return a consent form or leave any aspect of the consent form incomplete then the school will take this as a no.

Recorded

- When a parent/carer returns their consent form. This information should be entered into your School MIS.
- The consent form should then be filed away in a secure location for future reference if required.
- The consent form is being kept owing to it having the parent/carers signature which will allow the school to verify consent should they be challenged.

Managed

- The school will ask for very clear and specific consent for information not on the school consent form, should they require it, e.g. one-off events. This will be carried out using the same processes within this document.
- Any third-party controller who the school seek consent on behalf of will be named.
- If a parent/carer wishes to withdraw consent, they would contact the school and request a new consent form.
- This form will be sent out in a timely manner, and the School MIS updated accordingly.
- The new consent form will be filed with previous versions.
- Consent forms will be destroyed in accordance with the school personal data ecosystem.
- The school will avoid making consent a precondition of a service unless there is a lawful requirement to do so.

Subject Access

If the school receive a subject access request from an individual, they will follow the procedure listed below.

1. The school will contact the Data Protection Officer in the event of a subject access request and the Data Protection Officer will assist the school throughout the process.
2. The DPO will inform the school of the steps required to be carried out in regard to the Subject Access Request.
3. The school will first establish who the individual is making the request on behalf of. Is it access to their own personal data or is it on behalf of someone else?
4. The school will then establish if the individual has a valid reason for accessing the data. ICO guidelines state that they are not entitled to the information just because they may be interested.
5. If a valid reason is forthcoming, then the individual will be asked to make the request in writing. E-mail, fax and under certain circumstances social media are all acceptable for the subject access request to be a valid one.
6. The school may be allowed to charge a fee for the subject access request, and this will be communicated back to the individual if this is the case. However, this is unlikely, and the school will contact the DPO for further advice.
7. The school are not required to respond to verbal request. However, depending on the circumstances, it could be reasonable to do so, if the school are satisfied about the person's identity.
8. Should the individual requesting the data be disabled and they find it impossible or unreasonably difficult to make the request in writing, then the school will make reasonable adjustments under the equality act of 2010.
9. Even if the subject access request does not mention that it is a subject access the school will treat it as such, if it is clear that the individual is asking for their own personal data (or on behalf of someone else).
10. The subject access request will be treat as valid by the school regardless of who it has been sent to within the school.
11. The school will then establish if the information requested falls within the definition of personal data.
12. Once a valid subject access request has been received. The school will determine the nature of the request, and a decision will be made on what information can be provided if the subject access request relates to a child, and the time scales to adhere too. *GDPR states 1 calendar month for a request. However, ICO guidelines state 15 school days for a child's educational records.*
13. The school will provide the data as it was at the time of the request. Unless the routine use of the data has led to it being amended or even deleted. In this case the school would supply the information that it holds when the response is sent to the individual even if this is different to that held at the time of the request.
14. However, the school will not amend or delete any data during a subject access request that it would not have otherwise done so.
15. The school will provide the information to the individual in an 'intelligible form'. This means that it will be provided in a way that is capable of being understood by the average person.
16. The school may request more information about the subject access request if they are not satisfied that the person making the request is the individual to whom the personal data relates (or on behalf of), or the school may ask for information that the school reasonably needs to find the personal data covered by the request.

17. If the subject access request is made on behalf of a child, then the school will consider whether the child is mature enough to understand their rights and if so, the school will respond to the child not the parent. However, when considering borderline cases other factors will be taken into account.
18. The school will not comply with a subject access request if by doing so would mean disclosing information about another individual who could be identified from the information provided. Unless, the other individual has given consent, or it is reasonable in the circumstances to comply with the request without the individuals consent.

GDPR Individuals Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right of erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The school will ensure that all parents/carers and school staff are aware of these rights via the school privacy notices. Also, the school will ensure that should any parent/carer or member of school staff request to invoke any of the rights listed above, that they will treat the request in the correct manner and assist the individual anyway it can.

However, some of the rights listed will not apply due to other conditions set. An example would be the right to erasure, as if the individual requested this to happen to a record, then this could hamper the school's ability to perform its public task. As such, any requests that are made will be treat on a case by case basis, and the requester will be kept informed at all times around the decisions that the school make regarding their request.

Below is a brief guide to what each of the rights are:

1. **The right to be informed** – The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

2. **The right of access** – Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

3. **The right to rectification** – The GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete.

4. **The right to erasure** – The right to erasure is also known as the 'right to be forgotten'. The broad principal underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

5. **The right to restrict processing** – Individuals have the right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

6. **The right to data portability** – The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7. **The right to object** – Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise or official authority (including profiling). Direct Marketing and processing for purposes of scientific/historical research and statistics.

8. **Rights related to automated decision-making including profiling** – This is not applicable to schools. However, should an individual challenge the school in any way regarding automated decision making, then the school will carry out an investigation.

Vital Interests

GDPR has the following lawful bases for processing data:

(d) Vital interests: the processing is necessary to protect someone's life.

This is one of the lawful bases that the school uses for processing data within GDPR. It is required as the school processes the personal data to protect someone's life

This processing is necessary as without it the school would not be able to protect a person's vital interests in any other less intrusive way. The school rely on this basis to store medical and special educational needs data to assist the school in protecting someone's life.

Article 6 (1) (d) provides the lawful basis for processing where:

'Processing is necessary in order to protect the vital interests of the data subject or of another natural person'

Recital 46 provides further guidance:

'The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principal take place only where the processing cannot be manifestly based on another legal basis.'

This lawful basis generally only applies to matters of life and death. This is likely to be relevant for emergency medical care. While the school will use lawful basis **(a) consent: the individual has given clear consent for you to process their personal data for a specific purpose**, for the majority of its medical and special education needs processing. It may be required to use vital interests in the case of a life and death matter.

3rd Party Processing Agreement

STANDARD FORM CONTRACT TO ASSIST COMPLIANCE WITH OBLIGATIONS IMPOSED BY ARTICLE 17 OF THE DATA PROTECTION DIRECTIVE 95/46/EC

(FOR USE BY DATA CONTROLLERS AND DATA PROCESSORS LOCATED WITHIN THE EUROPEAN ECONOMIC AREA WHERE THE PARTIES HAVE ENTERED INTO A SEPARATE DATA PROCESSING AGREEMENT)

THIS AGREEMENT is made on [ ] 200[ ] BETWEEN:

(1) **[NAME]** (incorporated in, or existing and established under the laws of, [COUNTRY WITHIN THE EEA] whose registered office is at [REGISTERED OFFICE ADDRESS] (the "Controller"); and

(2) **[NAME]** (incorporated in, or existing and established under the laws of, [COUNTRY WITHIN THE EEA] whose registered office is at [REGISTERED OFFICE ADDRESS] (the "Processor").

BACKGROUND

(A) The Controller processes Personal Data in connection with its business activities;

(B) The Processor processes Personal Data on behalf of other businesses and organisations;

(C) The Controller wishes to engage the services of the Processor to process personal data on its behalf;

(D) Article 17(2) of the Data Protection Directive 95/46/EC (as hereinafter defined) provides that, where processing of personal data is carried out by a processor on behalf of a data controller the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;

(E) Articles 17(3) and 17(4) of the Data Protection Directive require that where processing is carried out by a processor on behalf of a controller such processing shall be governed by a contract or legal act binding the processor to the controller stipulating, in particular, that the processor shall act only on instructions from the controller and shall comply with the technical and organisational measures required under the appropriate national law to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing;

(F) In compliance with the above-mentioned provisions of Article 17 of the Data Protection Directive the Controller and Processor wish to enter into this processing security Agreement.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"Data Protection Directive" shall mean Directive 95/46/EC of the European Parliament and Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"national law" shall mean the law of the Member State in which the Processor is established;

"personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

"processing of personal data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

"sub-contract" and "sub-contracting" shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and "Sub Contractor" shall mean the party to whom the obligations are subcontracted; and

"Technical and organisational security measures" shall mean measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing.

2. CONSIDERATION

2.1 In consideration of the Controller engaging the services of the processor to process personal data on its behalf the Processor shall comply with the security, confidentiality and other obligations imposed on it under this Agreement.

3. SECURITY OBLIGATIONS OF THE PROCESSOR

3.1 The Processor shall only carry out those actions in respect of the personal data processed on behalf of the Controller as are expressly authorised by the Controller.

3.2 The Processor shall take such Technical and Organisational Security Measures as are required under its own national law to protect personal data processed by the Processor on behalf of the Controller against unlawful forms of processing. Such Technical and Organisational measures shall include, as a minimum standard of protection, compliance with the legal and practical security requirements set out in Appendix 1 of this Agreement.

4. CONFIDENTIALITY

4.1 The Processor agrees that it shall maintain the personal data processed by the Processor on behalf of the Controller in confidence. In particular, the Processor agrees that, save with the prior written consent of the Controller, it shall not disclose any personal data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

4.2 The Processor shall not make any use of any personal data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller.

4.3 The obligations in clauses 4.1 and 4.2 above shall continue for a period of five years after the cessation of the provision of services by the Processor to the Controller.

4.4 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

5. SUB-CONTRACTING

5.1 The Processor shall not sub-contract any of its rights or obligations under this Agreement without the prior written consent of the Controller.

5.2 Where the Processor, with the consent of the Controller, sub-contracts its obligations under this agreement it shall do so only by way of a written agreement with the Sub-Contractor which imposes the same obligations in relation to the security of the processing on the Sub-Contractor as are imposed on the Processor under this Agreement.

5.3 For the avoidance of doubt, where the Sub-Contractor fails to fulfil its obligations under any sub processing agreement, the Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this Agreement

6. TERM AND TERMINATION

6.1 This Agreement shall continue in full force and effect for so long as the Processor is processing personal data on behalf of the Controller.

6.2 Within [ ] days following termination of this Agreement the Processor shall, at the direction of the Controller, (a) comply with any other agreement made between the parties concerning the return or destruction of data, or (b) return all personal data passed to the Processor by the Controller for processing, or (c) on receipt of instructions from the Controller, destroy all such data unless prohibited from doing so by any applicable law.

7. GOVERNING LAW

7.1 This Agreement shall be governed by and construed in accordance with the national law of the Member state in which the Controller is established

AS WITNESS this Agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

SIGNED on behalf of [CONTROLLER]

(Authorised signatory)

(Print name and title)

SIGNED on behalf of [PROCESSOR]

(Authorised signatory)

(Print name and title)

CCTV Policy

1 Introduction

1.1 St Mary's Catholic school uses closed circuit television (CCTV) images to monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property.

1.2 The system comprises of 16 movable dome cameras and 61 fixed cameras; all Dome cameras are external only. This CCTV system is managed by our Site partners, Robertson FM.

1.3 The system does not have sound recording capability.

1.4 There are 3 units within our CCTV system which consist of 77 cameras.

1.5 The school CCTV system is monitored centrally from the FM Office and the school site manager is responsible for the monitoring of the CCTV.

1.6 The introduction of any changes to CCTV monitoring will be subject to consultation with staff and the school community.

1.7 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound (if applicable). All school operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

1.8 The school's CCTV information is logged in accordance with the school's GDPR personal data ecosystem.

2 Statement of Intent

2.1 The school complies with the Information Commissioner's Office (ICO) CCTV guidance to ensure it is used responsibly and safeguards both trust and confidence in its continued use.

https://ico.org.uk/your-data-matters/cctv/

2.2 A CCTV warning sign is clearly placed at the external entrance to the school.

2.3 The planning and design has endeavoured to ensure that our CTTV will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3 Siting the Cameras

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed, and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with GDPR and the Data Protection Act 2018.

3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

3.3 CCTV will only be used in classrooms for health and safety reasons. They will also be used in other areas within the school that have been identified as not being easily monitored.

3.4 Members of staff should have access to details of where CCTV cameras are situated, except for cameras placed for the purpose of covert monitoring.

4 Covert Monitoring

4.1 The school may in exceptional circumstances set up covert monitoring. For example:

4.1.1 Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
4.1.2 Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances, authorisation must be obtained from a member of the senior leadership team. Advice will also be sought from our Data Protection Officer.

4.3 Covert monitoring must cease following completion of an investigation.

4.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

5 Storage and Retention of CCTV images

5.1 Recorded data will not be retained for longer than is necessary. All images will be kept on the school site and will be overwritten every 30 Days unless they are required for an ongoing investigation. The only external viewing of CCTV images will be via Robertson FM based in FM Office. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All retained data will be stored securely.

6 Access to CCTV images

6.1 Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.

7 Subject Access Requests and Freedom of Information Requests

7.1 Individuals have the right to request access to CCTV footage relating to themselves under GDPR and the Data Protection Act 2018.

7.2 All requests are covered by the school Subject Access Request Policy and this can be provided on request.

7.3 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

7.4 CCTV is covered by the Freedom of Information Act 2000.

8 Access to and Disclosure of Images to Third Parties

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

8.2 The school will never disclose CCTV images to the media or place CCTV images on the Internet.

8.3 Requests should be made as described in paragraph 7.2.

8.4 The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

9 Complaints

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

School Photograph and Video Policy

The school will ensure that any photographs/videos used by the school will only be done so with explicit consent from the parent/carer of the child, or any adult included in the photograph/video. It is assumed by the school that this consent will only cover the image of the individual and does not include the publication of names, and any special category data such as gender and date of birth. The school will obtain further consent to use names, and special category data.

This will include photographs/videos;

used in school publications such as newsletters, prospectus;
used on the school website;
used on social media such as Facebook, twitter;
on school premises;
external venues.

The school will make parents/carers aware that while they are permitted to take photographs/videos during school performances/events, that these are for **private use** only, as long as they are not of an indecent nature.

Should any photographs/videos be shared without consent from the individuals within the photograph/video then they are breaking data protection laws, and the school reserve the right to report the breach of data protection to the Information Commissioners Office (ICO)

Parents/carers will be informed of this policy at every performance/event where the school believe that there is a possibility that photographs/videos could be taken. The school reserve the right to request that no photographs/videos are taken due to safeguarding concerns, which surpasses the parents/carer right to take photographs/videos for their own personal use.

Live streaming of school performances is strictly prohibited.

The above also includes performances/events that are not on the school site but include children and adults who attend the school.

Clear Desk Policy

To improve the security and confidentiality of information, we have adopted a Clear Desk Policy for Personal Identifiable Information (PII) throughout the school.

This will ensure that all Personal Identifiable Information (PII), is properly locked away or disposed of when not in use. The policy will reduce the risk of unauthorised access, loss of and damage to information during and outside of school hours.

This policy applies to anyone working within the school.

Whenever Personal Identifiable Information (PII) is not going to be used for an extended period the following will apply:

1. Must be removed from the area and locked away.
2. Must be shredded and must not be disposed in regular waste bins.
3. Keys for accessing drawers should not be left unattended.
4. Computers should always be locked when unoccupied.
5. Care should be taken when printing to ensure that documents are not left on the printer unnecessarily. Choose times to do this when printing may be less busy so the documents can be collected immediately. Under no circumstances should documents not be collected and left on the printer.

It is the responsibility of all staff working within the school to ensure their own compliance with this policy, failure to do so could lead to action being taken in accordance with the school data breach policy.