Data Protection Policy

St Joseph's
Catholic Primary School

ICO Registration Number
Z7976702

Complied By:	J Edwards
Approved by:	Governing Body
Review Date:	May 2018
Next Review Date:	May 2019
Revision Number :	6

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.
The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Andrew Wright and is contactable via dpo@stjosephs.harrow.sch.uk

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.
If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the School Records Management Policy.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. (See Appendix 6 for Subject Access Request Form). They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 30 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr J Grimes – Site Manager

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. (See Appendix 7) We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers
- Online on our school website or Learning Platform (DB Primary)

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Online Safety and Acceptable Use Policy and our Child Protection Policy for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices (See Appendix 1)
- Completing Privacy Impact Assessments (See Appendix 2) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices See Appendix 1)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- All passwords are set by LGfL and these are used to access school computers, laptops and the school email system. The viewing of passwords is only available to nominated contacts who have a USO-OTP (One Time Password) Second Factor Authentication Device.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB device
- Staff who have access to add, amend and delete personal information will sign and adhere to the Data Administrator Confidentiality Agreement. (See Appendix 3)
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online Safety and Acceptable Use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the personal data breaches procedure (See Appendix 4) and complete the Data Breach Record form. (See Appendix 5)

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of Information Publication Scheme
- Online Safety and Acceptable Use Policy
- Safeguarding/ Child Protection Policy
- School Records Management Policy

Appendix 1: Schools Privacy Notice

Privacy notice for Pupils and Parents/Carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, St Joseph's Catholic Primary School Dobbin Close Harrow HA3 7LP, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Andrew Wright (see 'Contact us' below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our School Records Management Policy sets out how long we keep information about pupils. To request a copy, please contact the data protection officer.

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so. Where it is legally required or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Our regulator e.g. Ofsted
- Diocese of Westminster
- Suppliers and service providers
- Central and local government
- Health and social welfare authorities and organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research. The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.
You can also contact the Department for Education with any further questions about the NPD.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer.

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please contact the Data Protection Officier.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to 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 us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

Andrew Wright dpo@stjosephs.harrow.sch.uk

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, St Joseph's Catholic Primary School Dobbin Close Harrow HA3 7LP are the 'data controller' for the purposes of data protection law.

Our data protection officer is Andrew Wright (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details & Identification Documents
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- 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
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- 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

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our School Records Management Policy

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority
- The Department for Education
- The Diocese of Westminster
- Your family or representatives
- Educators and examining bodies
- Our regulator e.g. Ofsted
- Suppliers and service providers
- Financial organisations
- Central and local government
- Health and social welfare authorities and organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:
- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to 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 us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

Andrew Wright dpo@stjosephs.harrow.sch.uk

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

Appendix 2: Privacy Impact Assessment Form

St Joseph's Catholic Primary School

Data protection impact assessment (DPIA) Form

As part of their responsibility under the GDPR, schools should conduct a DPIA in the following circumstances:

- When using new technologies.
- If the data processing is likely to result in a high risk to the rights and freedoms of individuals

Section A – DPIA screening questions

This section of the DPIA should be used to identify whether a DPIA is necessary. If any of the questions are answered 'Yes', it is a clear indicator that a DPIA should be completed. If you answer 'No' to any question, it should be clearly justified and evidenced as to why it is not applicable. These questions can also be used to clearly identify which potential risks are relevant and, therefore, contribute towards the structure of the DPIA.

Question	Yes	No	Unsure	Comments
Will the project involve collecting new information about individuals?				
Will the project require individuals to provide information about themselves?				
Will information about individuals be disclosed to other individuals or organisations who have not previously held information about the individual?				
Is any information about individuals held for purposes it is not currently used for, or in a way it is not currently used?				
Will the project involve using a new technology that might be perceived as being intrusive to an individual's privacy?				
Will the project result in any decisions or actions taken against individuals which may have a significant impact on them?				
Will any information about individuals raise privacy concerns, e.g. information they may wish to keep private, such as criminal information held on DBS certificates?				
Will the project require you to contact individuals in ways that they may find intrusive?				

The following three sections are designed to outline the specific need for the DPIA, once it has been identified as necessary using the screening questions above. This section should provide clarity on what the project will involve, the information required and the practical steps that will be taken to identify any risks.

Section B – Identify the need

Guidance • Explain what the project aims to achieve, and what the benefits will be to the school, to individuals and to other members of the school community. • Summarise why the DPIA was needed, in light of any questions that were answered 'Yes' within the 'DPIA screening questions' section. • Link to any other relevant documents related to the project, e.g. a project proposal.	

Section C – Provide the information flow

Guidance • Describe the process for the collection and deletion of any personal data. • Explain what information is used, what it is used for and who will have access to it. • Detail how many individuals are likely to be affected by the project.	

Section D – Practical Steps

Guidance • Explain what practical steps will be taken to ensure that all privacy risks are identified and addressed. • Detail who will be consulted internally and externally, and how this consultation will take place.	

Section E – Identify the risks

This section should be used to identify the specific privacy risks to individuals involved within a project, as well as compliance risks in relation to the GDPR and specific risks related to the school, e.g. reputational damage. All of these risks are usually overlapping – privacy risks to individuals may also lead to compliance risks, as well as risks to the school itself. Risks to individuals are categorised in many different ways, and it's important that all of these are considered and addressed – these can be related to physical safety, material damage, financial loss or emotional distress. For each question, you should tick either 'Yes', 'No', or 'Unsure', then provide additional information for each question to justify and explain your answer in the comments box.

Risks to individuals and the school

Question	Yes	No	Unsure	Comments
Will there be adequate disclosure controls in place to decrease the likelihood of information being shared inappropriately?				
Will the context in which the information is used change over time, leading it to be used for a purpose that the individual may not be aware of?				
Will the project involve the introduction of any new surveillance methods?				
Could the measures used to gain information from the individual be perceived as intrusive in any way?				
Will data be shared and merged between the school and other organisations? Is the individual aware of which information may be accessed?				
Will the project involve gaining information from individuals which may prevent them from remaining unidentified?				
Are individuals aware of the risks of identification and disclosure of information?				
Will gaining information mean that the school is no longer using information which is safely anonymised?				
Are appropriate procedures in place to ensure that information is not collected and stored unnecessarily, including ensuring that duplicate records are not created?				
Has an appropriate retention period been established?				

Risks to Compliance

	Question	Yes	No	Unsure	Comments
Principle 1 – personal data shall be processed fairly and lawfully	Have you identified the purpose of the project?				
	Is there a lawful reason you can carry out this project?				
	Have you identified the social need and aims of the project?				
	Are your actions a proportionate response to the social need?				
	Have you established a process for how you tell individuals about how their personal data is used and stored?				
	Do you need to amend your privacy notices?				
	Have you established which conditions for processing data apply to the project?				
	If sensitive personal data is involved, have you established which conditions for processing this data apply to the project?				
	If there is consent involved to use the personal data, is there an appropriate method in place for how this will be collected and what will be done if the data is withheld or withdrawn?				
	Will your actions interfere with the right to privacy, as outlined within the Human Rights Act 1998? If so, are the actions necessary and proportionate?				
	Question	Yes	No	Unsure	Comments
Principle 2 – personal data shall only be obtained for one or more specified and lawful purposes	Does the project plan cover all of the purposes for processing personal data?				
	Is there any personal data that could not be used, without compromising the needs of the project?				
	Question	Yes	No	Unsure	Comments
Principle 3 – personal data shall be adequate, relevant and not excessive	Is the quality of the information sufficient enough for the purposes it will be used?				
	Is there any personal data that could not be used, without compromising the needs of the project?				

	Question	Yes	No	Unsure	Comments
Principle 4 – personal data shall be accurate and, where necessary, kept up-to-date	If the procurement of new software is involved for the project, will it allow you to amend and delete information when necessary?				
	Have you ensured that personal data obtained from individuals and/or other organisations is accurate?				
	Question	Yes	No	Unsure	Comments
Principle 5 – personal data processed for a purpose shall not be held for longer than necessary	Have you established a suitable retention period for the personal data you will be processing? (outline how long you will keep the data for)				
	If you are procuring software, will this allow you to delete information in line with your retention periods?				
	Question	Yes	No	Unsure	Comments
Principle 6 – effective measures shall be taken against unlawful or unauthorised processing of data, and accidental loss, destruction of, and damage to, personal data.	Do any new systems provide protection against the security risks you have identified?				
	If the project involves a new system, are measures in place to ensure staff receive appropriate training and instruction, so they understand how to operate the new system correctly?				
	Have relevant staff received appropriate training and instruction relating to data protection and information sharing?				

Section F – identify privacy issues and risks

This section should be used to identify each privacy issue, and outline how the issue will affect individuals, the school or compliance with the GDPR – note that some privacy issues will not be applicable for all of these and may only cause risk to one or two. Each privacy issue should be provided with a reference number.

Reference number	Privacy issue	Risk to individuals	Risk to compliance	Risk to school

Section G – Identify and approve the solutions

In this section, you should assign each identified risk with a risk rating for the likelihood of it occurring, and the impact it would have on individuals using a scale of 1 (very little or no risk/impact) – 5 (extreme risk/impact). You should describe the actions you suggest should be taken to address the identified risks, as well as any future steps which would be necessary for the risk to be managed effectively. It should also be clear who is responsible for approving each solution.

You should also outline whether you will accept, reduce or eliminate each risk. It is important to note that not every risk needs to be eliminated completely – a DPIA seeks to reduce the impact of a risk to an appropriate level, whilst still allowing for the project to take place successfully. Where a risk has been accepted, you should explain the reasons for this.

Reference number	Risk(s) identified	Risk score	Solution(s)	Result	Evaluation	Approved by

Section H – Integrate the DPIA outcomes

Once risks and solutions have been identified, it is important that these are successfully integrated back into the overall plan for the project. This section should be used to identify who is responsible for actioning each solution and ensuring that the necessary action takes place. It is also important to identify who should be contacted for any future privacy concerns that may arise.

Using the same 1-5 scale as in section G, assign each action with an anticipated risk score in relation to the likelihood and impact of the risk occurring, once the action has taken place.

Reference number	Action to be taken	Date for action to be completed	Anticipated risk score following action	Responsibility for action (name and job role)	Current status

Contact for future privacy concerns

Name	
Job role	
Email address	
Telephone number	

Appendix 3: Data Administrator Confidentiality Agreement

Data Administrator Confidentiality Agreement

The school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore it is a data controller. Personal data can be processed in a paper format or an electronic format.
Your job role requires you to have access to the Data Systems we have in place to process personal data. When accessing and managing personal data you must at all times comply with the GDPR and DPA 2018. Use of the data must be consistent with the purpose for which the system was constructed. Data must be processed securely and not be subject to any unauthorised use or disclosure.

Staff who have the responsibility to access, add, amend and delete personal data must adhere to and comply with the following conditions:

- The data is to be used only for educational purposes and in the interests of the person to whom that data belongs, and not for any other purposes.
- Personal data is to be shared only with those who need the information to carry out an education function.
- Only authorised staff may access, add, amend and delete personal data on the data systems and they must never share their login details with anyone.
- Access to usernames and passwords is the responsibility of the nominated contacts in school who have a USO-OTP (One Time Password) Second Factor Authentication Device. Where necessary this responsibility may be shared with the system supplier (LGfL) and the system support supplier (Beebug)
- Paper-based records that contain personal data must be kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Personal data that is no longer needed must be disposed of securely. Personal data that has become inaccurate or out of date must also be disposed of securely. This includes shredding paper-based records and overwriting or deleting electronic files.
- Procedures should be in place to protect any data in transit. If data needs to be taken out of the system it must be in an encrypted form.
- Any breaches of data must be reported to the Data Protection Officer

Name:	
Role:	
Signature:	
Date:	

Appendix 4: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Data Breach Record Forms on the schools computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be on the school's computer system.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Appendix 5: Data Breach Record Form

St Joseph's Catholic Primary School

Data Breach Record Form

This form should be used to record any data breaches that occur in school. It should be completed by the school's Data Protection Officer (DPO) – the DPO is responsible for conferring with all individuals involved to ensure that all information recorded in this form is correct.

Contact Details	
Name of person who raised the issue:	
Contact email address of person who raised the issue:	
Contact telephone number of person who raised the issue:	
Job title:	
Date:	
Incident Information	
Date and time of data breach	
Description	
Type of Breach -Confidentiality -Availability -Integrity	
Categories of Individuals concerned	
Number of Individuals concerned	
Categories of personal records concerned	
Number of data records concerned	
Description of the likely consequences of the data breach.	
Action taken when breach was identified	
If breach was due to human error, name the member of staff and when they last received data protection training	
Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.	
Have persons affected been informed of the breach and when were they informed?	

Have persons affected been informed on how the breach will be rectified?	
Have any external bodies been informed of the breach, e.g. the ICO?	
Steps taken to prevent further data loss, including changes to existing procedure and refresher training given	
Conclusion	

By signing this form, the DPO agrees that the information within this form has been checked and is correct upon date of completion. All information in this form will be stored for school records so that the school can use the information to ensure their security systems are kept safe to minimise risks of a data breach.

Name of DPO:	
Signed (DPO):	
Date form completed:	

Appendix 6: Subject Access Request Form

St Joseph's Catholic Primary School
Subject Access Request Form

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them. Parents/carers can make a request with respect to their child's data and educational record where the child is under the age of 12. Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

Please complete this form and return it to the school.

School Details:
St Joseph's Catholic Primary School
Dobbin Close
Harrow
HA3 7LP

Name	
Relationship with the school. (Please tick as appropriate)	Pupil:
	Parent:
	Employee:
	Governor:
	Volunteer:
	Other: (Please specify)
Correspondence address	
Contact number	
Email address	
Details of the information requested (Please write here what information you would like and whether the information is about the child or parent)	

Appendix 7: Photographs Consent Letter and Consent Form

ST. JOSEPH'S CATHOLIC PRIMARY SCHOOL
Headteacher: Mr. P. SUTTON

DOBBIN CLOSE · HARROW · MIDDLESEX HA3 7LP
Telephone: 020 8863 8531 · Fax: 020 8863 3341 · e-mail: office@stjosephs.harrow.sch.uk
www.stjosephs.harrow.sch.uk

Dear Parents,

At St Joseph's, we sometimes take photographs of pupils. We use these on the school's website, on DB Primary, in the school newsletter, for media coverage and on display boards around the school.

We would like your consent to take photos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences. Please complete the form below and return it to the school.

If you change your mind at any time, you can let us know by emailing office@stjosephs.harrow.sch.uk , calling the school on 020-8863-8531, or just popping in to the school office.

If you have any other questions, please get in touch.

Many Thanks

Mr P Sutton
Headteacher

Photographs Consent

Child's Name: _____

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take photographs of my child. ☐

I am happy for photos of my child to be used on the school website. ☐

I am happy for photos of my child to be used on DB Primary. ☐

I am happy for photos of my child to be used in school newsletters. ☐

I am happy for photos of my child to be used in media coverage such as in the local newspaper. ☐

I am happy for photos of my child to be used in internal displays. ☐

I am **NOT** happy for the school to take or use photos of my child. ☐

Parent signature: _____Date:_____