# Data Protection Policy
# GDPR

## St Peter's Catholic Primary School

| | | |
|---|---|---|
| **Approved by:** | Governing Body | **Date:** Autumn 2025 |
| **Last reviewed on:** | Autumn 2025 | |
| **Next review due by:** | Autumn 2026 | |

## Contents

# 1. Aims

St Peter's Catholic Primary 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), the UK-GDPR (the UK government's Data Protection, Privacy and Electronic Communications (EU Exit) Regulation) and the provisions of the Data Protection Act 2018 (DPA 2018).

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). It also reflects the ICO's code of practice for subject access requests and 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. The data controller

St Peter's Catholic Primary 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. Our ICO registration number is Z4981417.

# 4. 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.

## 4.1. Governing body

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

## 4.2. 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 body and, where relevant, report 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.

Our DPO may be contacted via the school office or by email to is Data Tools for Schools Limited, contactable via the school office at office@stpeters-leatherhead.surrey.sch.uk.

## 4.3. Headteacher

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

## 4.4. 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

## 5. 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.

## 6. Data protection by design and default

Our school 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 xx)
- Completing privacy impact assessments 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)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- 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)
    - 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

# 7. Collecting personal data

## 7.1. Lawfulness, fairness and transparency

St Peter's Catholic Primary School will only process personal data where we have one of '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 meet one of the special category conditions for processing which are set out in the Data Protection Act 2018. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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's **Record Retention Schedule**.

# 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 share personal data with statutory bodies, such as the Department for Education and Local Authority where we are required to do so.

We will also share personal data with law enforcement agencies 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 should be submitted in writing, either by letter, email or fax to the DPO via the school office at office@stpeters-leatherhead.surrey.sch.uk. 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. Other data protection rights of the individual

In addition to the right to make a subject access request (see above),individuals also have the right to:

- Access to their supplementary information
- 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)

### 9.3. 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.

### 9.4. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or voluminous. We will inform the individual of this within one 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.

## 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 15 school days of receipt of a written request.

## 11. 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. 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 magazines, brochures, newsletters, etc.

- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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 Safeguarding and Child Protection Policy for more information on our use of photographs and videos.

## 12. 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
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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 E-Safety Policy/ICT policy/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)

## 13. 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.

## 14. 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 procedure set out in Appendix 1. 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

## 15. Data use and access act 2025

The Data Use and Access Act 2025 (What it means for schools)

New legislation has been introduced to modernise how data is used and accessed. It is designed to supplement and clarify the UK GDPR and can be applied to requests received since January 2024. The key implications for schools are as follows:

Timescale - the one-month time requirement starts once the data subject's identification has been confirmed. If the school needs to clarify the scope of a data search (what the data subject is asking for), the 'clock' is paused until clarification has been received from the data subject.

Scope of the search - the law clarifies that requests for personal data must be 'reasonable and proportionate'. The school DPO will provide advice and guidance to assist the data subject (and the school) to identify what information meets the 'reasonable and proportionate' requirement. This will avoid having a scope that is so broad that it puts undue pressure on school resources and delays the time in which the data subject can access the data they need.

Information already held - the law clarifies the principle that the school does not need to send information to the requester, which they already hold or have access to. This confirms there is no requirement to send copies of emails and letters that were communicated by the school to and from the data subject.

Data Protection Complaints procedure - schools must have a dedicated data protection complaints procedure. Complaints about how the school has managed its data protection responsibilities must be acknowledged within 30 days and should be processed without undue delay.

The school's Data Protection Complaint Procedure is managed by its DPO. The complaints procedure can be found on the DPO website (RSimmonsLtd.com), or by following the link below:
https://www.rsimmonsltd.com/making-a-complaint

The DPO will support the Data Protection Complaint Procedure in respect to the school and the data subject. In the first instance the data subject should read the information titled 'Making a Data Protection Complaint about a school' on the DPO website. A complaint can then be made via a Microsoft Form or via a downloadable word document

## 16. 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.

## 16. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **annually** and shared with the full governing body.

## 17. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online safety Policy
- Acceptable Use Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct

# Appendix 1: Definitions

| Term | Description | Example |
|---|---|---|
| Data subject | The person that the data relates to. | John Smith the pupil.<br>Jane Smith the teacher. |
| Data item | A single piece of information about a data subject. | "Ethnicity = white British"<br>"Attendance = 97%" |
| Data item group | A group of data items that are typically captured about the same activity or business process in school.<br>These are also sometimes called data elements or data scope within the data community/sharing agreements schools have with suppliers. | Behaviour management, or catering. |
| Dataset | A collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. | A database, table, number of related tables, a spreadsheet |
| System | A piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life. | Capita SIMS, ParentPay, MyMaths. |
| System group | An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside. | Core MIS, payments, curriculum tools |
| Personal data | Information relating to a natural identifiable person, whether directly or indirectly | John Smith was born on 01/01/1990.<br>The head teacher's salary is £60,000. |
| Special category data | These are highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons you need to have to access and process that information.<br>In education, it would also be best practice to treat things like FSM, SEN, and CIN/CLA status as special category data. | Tightly defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership, and health or sex life. Data relating to criminal offences is also afforded similar special protection. |
| (Data) Controller | The organisation who (either alone or in common with other people or organisations) determine the purpose for which, and the manner in which data are processed. | A school is usually the data controller, but they can also be a joint controller with their LA or DfE. |
| (Data) Processor | A person or organisation who process data on behalf of and on the orders of a controller. | A catering supplier the school uses. |

| Term | Description | Example |
|---|---|---|
| Data audit/data asset register | The assessment of data and its quality, for a specific purpose. Other terms you might hear are data map or information asset log. In this context, we simply want the list of personal data assets that we hold, from which we can go on to place further important information alongside | |
| Lawful basis and conditions for processing | These are the specific reasons, set out in law, for which you can process personal data. There is one list for personal data (lawful basis article 6) and another list for processing special category data (article 9). | "The processing is necessary for administering justice, or for exercising statutory or governmental functions. |
| Data retention | How long you will hold information to do the processing job you need it for. At the end of a data retention period, processes should be in place to ensure it is properly disposed of. | "We keep parent's phone numbers until 1 month after they leave the school in case of any issues that need resolving (for example, payment or repayment of lunch money) and then it is deleted." |
| Privacy notice | This is a document that explains to the people you have data about ("data subjects") the data items you hold, what they are used for, who it is passed onto and why, and what rights they have. | DfE publish model privacy notices. |
| Subject Access Request (SAR) | This is where a person (data subject), requests access to the information you hold about them. Timescales for responding, as well as reasons why you must comply, or may refuse, are set out in law. A Subject Access Request is can be for all data about a subject or for specific information. | "I want to know the attendance data you hold about my son" |
| Data Protection Impact Assessment (DPIA) | This is a process to consider the implications of a change you are introducing on the privacy of individuals' data. Assessing privacy at the outset helps you plan consultation / awareness / consent type options from the outset. "Privacy by design" is a term that is used in this space. | You would undertake one of these if introducing a new system to use fingerprinting within catering provision. |
| Data breach | A personal data breach means the accidental or unlawful destruction, loss, alteration, disclosure, or access to, personal data. Breaches are either accidental or deliberate. It also | Sending a list of pupil names, attainment marks and dates of births to the wrong school. |

| Term | Description | Example |
|---|---|---|
| | means that a breach is more than just about losing personal data. | |
| Automated decision making/profiling | This is when machines/software make decisions based on rules generated by the machine/software, without human intervention, about someone. Typically, it is the significance of the decision that drives the caution and concern here. | "Anyone recorded as attendance >99% will get a voucher for X" |
| Data Protection Officer (DPO) | The GDPR requires data controllers to designate a Data Protection Officer (DPO)<br>The DPO must be entrusted with the following:<br>(a) informing and advising the controller (including processors and employees) of their data protection obligations<br>(b) providing advice on data protection and monitoring compliance<br>(c) co-operating with the Information Commissioner, acting as the contact point for issues relating to data protection.<br>(d) monitoring compliance with policies of the controller in relation to the protection of personal data | The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.<br>A DPO can be an existing employee or externally appointed. Ideally, an effective DPO will have significant skills and knowledge of the education system and its regulations.<br>When deciding on appointing or designating a DPO, you must keep in mind that there are no 'certified DPOs' yet with respect to GDPR in the UK. |

# Appendix 2: Personal data breach procedure

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

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO via office@stpeters-leatherhead.surrey.sch.uk
2. 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
3. The DPO will alert the headteacher and the chair of governors
4. 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. (Actions relevant to specific data types are set out at the end of this procedure)
5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
6. 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 is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

7. 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 electronically in the Data Protection folder.
8. 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:
        i. The categories and approximate number of individuals concerned

ii. 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

9. 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

10. 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

11. 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

12. 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 stored electronically in the Data Protection Folder.

13. 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

**Actions to minimise the impact of data breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

**Sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach which would incur a similar response:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked, and parents' financial details stolen

## Appendix 3: Data breach report form

# Data Breach Report Form

This form should be completed as soon as a data breach has been discovered. Please complete sections 1 -7 with as much information as possible and pass the form on to the School Business Manager or Headteacher immediately. The breach will be recorded on the School's Breach Register and the DPO informed so that an investigation can be carried out.

| | | |
|---|---|---|
| | Report by: | |
| | Date | |
| 1 | Nature of breach e.g. theft/disclosed in error/technical problem | |
| 2 | Description of how breach occurred: | |
| 3 | When was the breach reported and how did you become aware? | |
| 4 | Full description of all personal data involved | |
| 5 | Number of individuals affected?<br>Have all individuals affected been informed? | |
| 6 | What immediate remedial action was taken: | |
| 7 | Has the data been retrieved or deleted? If yes – date and time: | |
| 8 | Any Procedure changes needed to reduce risks of future data loss | |
| 9 | Conclusion | |

# Appendix 4: Subject Access Request Form

Personal information collected from you by this form is required to enable your request to be appropriately processed. This personal information will only be used in connection with the processing of this Subject Access Request.

This form is only to be used when making an application for personal data held by St Peter's Catholic Primary School.

**Please note: Before logging your request, we will require proof of identity by production of a passport, photo-driving licence, or a utility bill in your name and current address. Please supply your proof of identity when making your application. A scanned or photocopied copy will be sufficient.**

| | |
|---|---|
| Name | |
| Address | |
| Previous Address: (If Applicable) | |
| Date of Birth: | |
| Contact Phone number: | |
| Email Address: | |
| Details of information requested (please specify the date range that you require information for) : | |

**Parent applying on behalf of a child**

If you are a parent applying for access on behalf of your child, please complete the following and tick the relevant box.

*Please note that you must be able to establish that you are legally able to act on behalf of your child. This generally means that you must have parental responsibility for him or her. It should be noted that a parent can only be granted access to their child's records if this is considered to be in the child's interests.*

| | |
|---|---|
| Name of child | Date of Birth |

I (Name of parent) ..... am making a request for access to records on behalf of the child named above and:

Tick as appropriate:

- ☐ The child is incapable of understanding the request and I am making the request on his/her behalf ☐
- ☐ The child has consented to my making this request on his/her behalf and this consent was freely given ☐

| Childs signature (where consent is given) | Date |
|---|---|
| | |

**Applicants signature**

I declare that the information given be me is, to the best of my knowledge correct and that I am entitled to apply for access to the information referred to above, under the terms of the Data Protection Act 1998.

| Signature: | Date of Request: |
|---|---|
| | |

Once St Peter's Catholic Primary School has received all the required information, your request should be completed within the one month statutory reply period. In exceptional circumstances where it is not possible to comply within this period you will be informed of the delay and given a timescale for when your request is likely to be met. Please return this form to:

St. Peter's Catholic Primary School
Grange Road
Leatherhead
Surrey
KT22 7JN

Please note:

- ☐ The school may contact you for further clarification regarding the information required.
- ☐ Once the information has been collated, you will be notified that your file is ready for collection or to be sent securely.

**For schools use only**

| Form of ID Provided | Date Request Received |
|---|---|
| Date Request Acknowledged | Target Date for Completion of SAR |

# Appendix 5: Photographic Images of Children – Consent Form

**Consent form 2025 - 2026**

Child's name: ……..

Class: ……...

| **Activities** | Yes | No |
|---|---|---|
| I give permission for my child to take part in local school trips.<br>(the church, local area, swimming, another local school) | | |
| **Photographs** | | |
| I give permission for my child's photograph to be used in the school newsletter or prospectus. | | |
| I give permission for my child to have individual and class photographs taken. | | |
| I give permission for my child's photo to be used on the school website. | | |
| I give permission for my child's photograph to be used on open day posters. | | |
| I give permission for my child's photograph to be featured on the school Facebook page. (@Stpeters70) | | |
| I give permission for photos/videos of my child to be used in training events for other teaching professionals.<br>(e.g. pictures of children's work, classroom clips etc) | | |
| I give permission for my child's photograph to appear in local newspapers e.g. leavers supplement or coverage of local events. | | |
| **Newsletter** | | |
| I give permission for my child's name (first name only) to be used in the school newsletter. | | |
| **PG films** | | |
| I give permission for my child to watch PG rated films within school.<br>(the class teacher will always notify parents in advance of the title of the film) | | |

Signed: ……
(parent/carer)

Date: ……

If you would like to amend or withdraw your permission you can do so at any time by emailing Mrs Hall deputy@stpeters-leatherhead.surrey.sch.uk

# Appendix 6: Retention of records schedule

**Retention Guidelines**

- Instrument of Government (life of school)
- Parent and staff governor election records (6 months)
- Appointment of co-opted governors (end of term)
- Appointment of the clerk (6 years)
- Declarations against disqualification (6 years)
- Induction programme (end date + 6 years)
- Records relating to DBS (date of check + 6 years)
- Scheme of Delegation & terms of reference (until superseded)
- Minutes and agendas (life of school)
- Reports to governors (kept with minutes)
- Register of attendance (6 years)
- Governor Monitoring visit reports (3 years)
- Records of chairs election (kept with minutes)
- Complaints investigated by board (6-40 years)
- Policy documents (until superseded)

**The school must ensure they have:**

- Signed copies filed in school
- Pandemic copies signed and filed
- Supporting paperwork including agenda filed with minutes
- Confidential minutes filed separately (until information in the public domain)
- Signed copies are kept securely with limited access
- Copy requests protocols in place