St Augustine's Catholic Primary School

Data Protection Policy

April 2021

Data Protection Policy

Contents

1. Aims

St Augustine's Catholic Primary School aims to ensure that all personal data collected about employees or their families, pupils, parents/guardians, governors, visitors, business partners and other individuals is collected, stored and processed in accordance with the Data Protection Act (DPA) 1998, the General Data Protection Regulation (UK GDPR) and the new Data Protection Act (DPA) 2018 and with other relevant legislation.

This policy relates to all St Augustine's Catholic Primary School employees (including voluntary, temporary, contract and seconded employees) who capture, create, store, use, share and dispose of information on behalf of St Augustine's Catholic Primary School. These persons shall be referred to as 'users' throughout the rest of this policy.

St Augustine's Catholic Primary School shall be referred to as 'the school' or 'we' throughout the rest of this policy.

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. 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.

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
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 • Health – physical and mental
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

We process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore we are a data controller.

We are 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 St Augustine's Catholic Primary School and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

- **Board of Governors**

Our Board of Governors have overall responsibility for ensuring that we comply with all relevant data protection obligations.

- **Data Protection Officer**

The data protection officer (DPO) is responsible for overseeing the implementation of this policy. The DPO is the first point of contact for individuals whose data we process, and for the ICO.

Our DPO is Louise Fishwick and is contactable at bursar@st-augustines-pri.lancs.sch.uk

- **Headteacher**

Our Headteacher acts as the representative of the data controller on a day-to-day basis.

- **All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the DPO 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, require a privacy notice or receive a data protection rights query
    - 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 we must comply with. The principles of DPA and GDPR state that personal data/information 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 we aim to comply with these principles.

7. Collecting personal data

- **Lawfulness, fairness and transparency**

We will only process personal data where we have a 'lawful basis' (legal reason) to do so under data protection law:

- The data needs to be processed so that we can **fulfil a contract** with the data subject
- The data needs to be processed so that we can **comply with a legal obligation** (e.g. The Education Act 1996, School Standards and Framework Act 1998, Education Act 2002, Children and Families Act 2014)
- The data needs to be processed to ensure the **vital interests** of the data subject or another person e.g. to protect someone's life
- The data needs to be processed so that we can perform a task **in the public interest**
- 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.

- **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 Records Retention 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 who 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
- Emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

9. Subject access requests and other rights of individuals

- **Subject access requests**

Individuals have a right to make a 'subject access request' to gain access to personal information that we hold 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 or email to the DPO. 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.

- **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 calendar month of receipt of the request
- Will provide the information free of charge; however, we may charge for further copies or where requests for information are unfounded or excessive.
- 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. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

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

- **Other data protection rights of the individual**

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

- Be informed via privacy notices
- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data; inaccurate or incomplete data must be rectified within one month
- Object to their personal data being used for profiling, direct marketing or research purposes
- Challenge processing which has been justified on the basis of public interest
- 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 provided in a structured, commonly used, machine-readable format when asked

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, can request to have access to their child's educational record (which includes most information about a pupil). Such requests should be made directly to the school.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals. 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.

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.

12. 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)
- Completing privacy impact assessments where the processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- 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 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

13. 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 securely 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, authorisation must be obtained from the Headteacher
- 'Strong' passwords are used to access school networks, 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
- 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)

14. 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 (if we cannot or do not need to rectify or update it).

15. Personal data breaches

We 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.

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.

17. Monitoring arrangements

The Headteacher is responsible for monitoring and reviewing this policy **every 2 years** and shared with the full governing board.

18. Summary of requirements

In order to comply with these principles and meet all data protection obligations as stipulated in data protection legislation, the school will:

- Raise awareness of data protection across the school.
- Offer data protection training to all employees and governors.
- Create a data protection policy for the school that is updated bi-annually.
- Complete a personal data processing audit, which lists the following:
    - Name of the personal data set.
    - Purpose for processing this personal data set.
    - Who the data set is shared with.
    - If the data is transferred to another country.
    - How long we keep the personal data set (retention).
    - The technical and organisational security measures to protect the personal data set.
    - The legal basis for processing as described above.
    - If consent is the legal basis for processing, details of the evidence of this consent.
- Put any risks found from the personal data processing audit process into a risk register.
- Review the school's consent forms so they meet the higher standards of GDPR, create an audit trail showing evidence of consent.
- Under 13's can never themselves consent to the processing of their personal data in relation to online services, this rule is subject to certain exceptions such as counselling services.
- Register with the Information Commissioners Officer as a data controller.
- Appoint a Data Protection Officer
- Create a privacy notice that will let individuals know who we are, why we are processing their data and if we share their data.
- Create a policy/procedure to allow data subjects to exercise their rights:
    - to be informed via a privacy notice.
    - of access via a subject access request within 1 month.
    - of rectification to incorrect data within 1 month.
    - to erasure unless there is a legal reason for processing their data.
    - to restrict processing to the bare minimum.
    - to data portability to receive their data in the format they request.
    - to object to personal data being used for profiling, direct marketing or research purposes.
    - in relation to automated decision making and profiling.
- Check any business contracts with suppliers to ensure that they will conform to new data protection legislation.
- Implement technical and organisational controls to keep personal data secure.
- When required, use Privacy Impact Assessments to assess the privacy aspects of any projects or systems processing personal data.
- Investigate all information security breaches, and if reportable, report to the Information Commissioners Office within 72 hours.
- Undertake data quality checks to ensure personal data is accurate and up to date.
- Demonstrate our compliance through audits, spot checks, accreditations and performance checks.

Appendix 1: 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
- The DPO/Headteacher 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)
- The DPO/Headteacher will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO/Headteacher 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/Headteacher 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
    - 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.
- 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 stored.
- 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 above 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.