

St. Patrick's Catholic Primary School



Data Protection Policy

Item	Details
School / trust name	St. Patricks Catholic Primary School
ICO registration number	ZB196565
Data Protection Officer	Intergence Lead Contact: Rupert Ogilvie dpo@stpatricksprimary.org.uk
Approved by	Finance Committee Governing board October 2026
Next review	October 2028

1. Aims and scope

St. Patrick's collects, stores and uses personal data about pupils, parents and carers, staff, governors, volunteers, visitors and others to carry out its functions. We aim to do this lawfully, fairly and transparently, and to keep that data secure.

This policy applies to all personal data we process, in any format (paper, electronic, images, audio and video), wherever it is held. That includes school systems, cloud services, school-issued devices and, where permitted, personal devices.

It applies to all staff, governors, trustees, volunteers, contractors and anyone else who handles personal data on the school's behalf. A breach of this policy may lead to disciplinary action.

2. Legislation and guidance

This policy meets the requirements of:

- the [UK General Data Protection Regulation](#) (UK GDPR)
- the [Data Protection Act 2018](#) (DPA 2018)
- the [Data \(Use and Access\) Act 2025](#) (DUAA), including the subject access and lawful basis changes in force from 5 February 2026 and the complaints duty in force from 19 June 2026
- the [Privacy and Electronic Communications Regulations 2003](#) (PECR), for cookies and electronic marketing
- the [Protection of Freedoms Act 2012](#), sections 26 to 28, for biometric data

- the [Education \(Pupil Information\) \(England\) Regulations 2005](#), for parental access to the educational record (maintained schools)

It also follows ICO guidance, including the ICO's [video surveillance guidance](#), the DfE's [Data protection in schools](#) guidance and Keeping Children Safe in Education.

3. Definitions

Term	Meaning
Personal data	Any information relating to an identified or identifiable living person (the data subject), such as a name, ID number, location data, online identifier, photo or assessment record.
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health, sex life or sexual orientation.
Criminal offence data	Data about criminal allegations, proceedings, convictions or related security measures, for example DBS check outcomes.
Processing	Anything done to personal data, including collecting, recording, organising, storing, using, sharing, erasing or destroying it.
Data subject	The person the personal data is about.
Data controller	The organisation that decides why and how personal data is processed.
Data processor	An organisation or person that processes personal data on the controller's instructions, for example an MIS or payments provider.
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, roles and responsibilities

St. Patrick's is the data controller for the personal data it processes. It is registered with the ICO and pays the annual data protection fee (registration number: ZB196565).

Governing board The board has overall responsibility for compliance with data protection law. It approves this policy and receives at least an annual report from the DPO.

Data Protection Officer (DPO). Intergence :The Old Coach House, Brewery Road, Pampisford, Cambridge, CB22 3HG Lead Contact: Rupert Ogilvie
dpo@stpatricksprimary.org.uk

The DPO:

- informs and advises the school and its staff on their data protection obligations
- monitors compliance, including audits, training and records of processing
- advises on and reviews data protection impact assessments (DPIAs)
- is the first point of contact for data subjects and for the ICO

- reports directly to the governing board, operates independently and is given the resources needed for the role

Headteacher. Acts as the representative of the controller day to day and makes sure the school has the people, systems and procedures to comply.

The Senior Admin Officer The in-school contact for the DPO. Maintains the information asset register, breach log and request log.

All staff must:

- collect, store and process personal data in line with this policy
- tell the school promptly about changes to their own personal data
- contact the DPO or data protection lead if they are unsure of the lawful basis for something, need to rely on consent, need to share data outside the school, are starting a new system or project that uses personal data, or need to transfer data outside the UK
- report any actual or suspected data breach **immediately** (see section 15)
- pass any request from an individual about their data to the data protection lead **on the day it is received**

5. Data protection principles

Article 5 of UK GDPR sets out seven principles. The school will make sure personal data is:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes, and not used in a way incompatible with them
3. adequate, relevant and limited to what is necessary
4. accurate and, where necessary, kept up to date
5. kept for no longer than is necessary
6. processed securely, protecting against unauthorised or unlawful processing, loss, destruction or damage

The seventh principle is **accountability**. The school must be able to show that it complies. We do this through this policy, records of processing activities (ROPA), DPIAs, data processing agreements with suppliers, training records, and logs of breaches, requests and complaints.

6. Lawful bases, special category data and consent

We will only process personal data where we have one of the lawful bases in Article 6 of UK GDPR. For a school these are usually:

Lawful basis	Typical school examples
Public task	Teaching, assessment, attendance, pastoral care, school census returns
Legal obligation	Safeguarding, staff right-to-work and pre-employment checks, reporting to the DfE and local authority
Contract	Staff employment contracts, contracts with suppliers
Vital interests	Sharing medical information with paramedics in an emergency

Lawful basis	Typical school examples
Consent	Photos on social media, some marketing, optional biometric systems
Legitimate interests	Only for activities outside our public tasks, such as some fundraising or lettings, and only after a balancing test

The DUAA added a “recognised legitimate interests” basis (for example, safeguarding and emergencies). For most school safeguarding work, legal obligation or public task remains the correct basis. The DPO will advise if another basis may apply.

Special category and criminal offence data. Processing these also needs an Article 9 condition (such as substantial public interest for safeguarding, employment obligations, or explicit consent) and, where the DPA 2018 requires it, an **appropriate policy document** setting out how we comply. [Link to the school’s appropriate policy document.]

Further processing. Using data for a new purpose is only allowed where it is compatible with the original purpose, permitted by law, or the individual has consented. We will update our privacy notices before doing so.

Consent. Consent must be freely given, specific, informed, unambiguous and recorded. It can be withdrawn at any time, as easily as it was given. We will not rely on consent where another basis applies, because a pupil or employee may not feel free to refuse.

Children and consent. For online services offered directly to children, a child aged 13 or over can give their own consent. For younger children we seek consent from a parent or carer. More generally, we consider pupils aged around 12 and over mature enough to understand and exercise their own data rights, assessed case by case.

7. Privacy notices, data minimisation and accuracy

We tell people how we use their data through privacy notices for pupils (in age-appropriate language), parents and carers, staff, governors and volunteers, job applicants and visitors. Notices are published on [the school website] and provided at the point data is collected. They explain our lawful bases, who we share data with, how long we keep it, individuals’ rights, and how to complain to us and to the ICO.

We only collect the personal data we need for the stated purpose. Staff must not collect extra data “just in case”.

We ask parents and staff to check and update their contact and medical details at least [annually / at the start of each school year], and we correct inaccurate data promptly when told about it.

When data is no longer needed, it is deleted or securely destroyed in line with our retention schedule (section 13).

8. Sharing personal data

We do not normally share personal data without a lawful basis and, where appropriate, telling the individual first. We may share it where:

- there is a safeguarding concern or a risk to the safety of a pupil or someone else
- we are required to by law, for example for the school census or by the Department for Education, the local authority, Ofsted, exam boards, HMRC or the police

- we need to work with other agencies supporting a pupil, such as health services or social care
- suppliers or contractors need data to provide services to us, such as our MIS, catering, IT or trip providers

Safeguarding. Data protection law does not prevent, or limit, the sharing of information to keep children safe. Staff who have a safeguarding concern must follow the child protection policy and speak to the Designated Safeguarding Lead without delay. Concern about breaching data protection is never a reason to withhold information that could protect a child.

Suppliers (processors). Before sharing data with a supplier, we will:

- choose only suppliers that give sufficient guarantees of data protection compliance
- put a written data processing agreement in place that meets Article 28 of UK GDPR
- share only the data needed for the service

We may also share data with emergency services and local authorities to help them respond to an emergency affecting pupils or staff.

9. Individual rights and subject access requests

Individuals have the right to:

- access their personal data (a subject access request, or SAR)
- be told how their data is used (the right to be informed)
- have inaccurate data corrected (rectification)
- have data erased in certain circumstances
- restrict processing in certain circumstances
- object to processing, including direct marketing
- data portability, where processing is based on consent or contract and carried out by automated means
- not be subject to solely automated decisions with legal or similarly significant effects without safeguards, including the right to human review
- complain to the school and to the ICO

Making a subject access request

A request can be made verbally or in writing, to any member of staff, and does not have to mention data protection. Staff must pass it to the data protection lead the same day. Using our [SAR form] helps but is not required.

How we respond

1. **Log and acknowledge** the request on the day it reaches the data protection lead.
2. **Verify identity** where we are not sure who the requester is, using proportionate checks.
3. **Clarify if needed.** If we reasonably need more information to find the data, we will ask. The time limit is paused until the requester replies.
4. **Search.** We will carry out a reasonable and proportionate search for the information requested.
5. **Review and redact** third-party information and anything covered by an exemption. Examples include information likely to cause serious harm, safeguarding records where disclosure is not in the child's best interests, legally privileged material,

references given in confidence, exam scripts and, until results are published, exam marks.

6. **Respond within one calendar month** of receipt. We may extend this by up to two further months where requests are complex or numerous. If so, we will tell the requester within the first month and explain why.

Responding to a SAR is free of charge. Where a request is manifestly unfounded or excessive, we may charge a reasonable fee or refuse it. We will explain why and tell the requester of their right to complain to the ICO. School holidays do not extend the deadline, so the school will make sure SARs can be handled during closure periods.

Pupils' rights

Personal data about a child belongs to that child, not their parents. Where a pupil is mature enough to understand their rights (generally from around age 12, assessed case by case), a SAR made by a parent on their behalf needs the pupil's consent or another good reason. For younger pupils, parents can usually exercise these rights on their behalf.

10. Parental access to the educational record

Parents, or those with parental responsibility, have a right to free access to their child's educational record within **15 school days** of a written request, under the Education (Pupil Information) (England) Regulations 2005. A charge may be made for a copy, up to the cost of supply. This right belongs to the parent, is separate from a SAR, and applies regardless of the child's age.

The same exemptions apply. We will not disclose information that could cause serious harm or that a court has ordered must not be shared.

11. Biometrics, CCTV, photographs and video

Biometric recognition systems: None in use at St. Patricks

CCTV

We use CCTV at around the outside of the school for [the safety of pupils, staff and visitors, and the security of the site]. Signs make clear that CCTV is in use. Cameras do not cover areas where people expect privacy, such as toilets or changing rooms. Footage is kept for [30] days unless needed for an investigation, and access is restricted to SLT. A DPIA covers the system, and requests for footage are handled as SARs.

Photographs and video

We take photographs and videos of pupils for teaching, assessment and safeguarding (public task) and, with consent, for communication and promotion. We ask [parents / pupils aged 13 and over] for consent to use photographs:

- within school, on noticeboards and in school publications
- outside school, in newsletters, the press and on the school website
- on social media

We do not name pupils alongside their photographs without separate consent. Consent can be withdrawn at any time. We will remove photographs where we can, but cannot recall material already printed. Staff take photographs on school devices only, unless [stated exceptions].

Parents filming school events for personal use is not covered by data protection law, but we will ask them not to post images of other children online.

12. Data protection by design, DPIAs, AI and educational technology

We build data protection into everything we do. This means:

- appointing a suitably qualified DPO and giving them the resources they need
- processing only the data needed for each purpose
- completing a **data protection impact assessment (DPIA)** before any new processing likely to be high risk, for example a new MIS, CCTV, biometrics, large-scale use of special category data, monitoring software, or a new AI tool that processes pupil or staff data
- building data protection into our policies, training and contracts
- keeping a record of processing activities and an information asset register

AI tools and educational technology

Staff must not enter personal data about pupils, parents or colleagues into any AI tool or online service that the school has not approved. Before approving a tool, [the DPO / data protection lead] will check:

- what data it collects, where it is stored and whether it is used to train the provider's models
- whether a DPIA is needed and a data processing agreement is in place
- whether it meets the DfE's [Generative AI: product safety expectations](#) and data protection standards

No significant decision about a pupil or member of staff will be made solely by automated means without meaningful human involvement. [Link to the school's AI / acceptable use policy.]

13. Data security, storage and retention

We protect personal data against unauthorised or unlawful access, alteration, processing, disclosure, accidental loss, destruction or damage. In particular:

- paper records containing personal data are kept in locked cabinets or rooms when not in use, and are not left on desks, staffroom tables or noticeboards
- staff do not take paper records or portable media containing personal data off site without [the data protection lead's] approval, and keep them secure while away
- school accounts use strong passwords and **multi-factor authentication**, devices lock automatically and school laptops are encrypted
- staff use school-approved systems (for example, [Microsoft 365 / Google Workspace]) to store and share data, not personal email, personal cloud storage or USB sticks
- staff, pupils and governors using personal devices follow the [acceptable use / BYOD] policy
- emails containing sensitive data are sent securely, recipients are checked before sending, and BCC is used for group emails to parents
- access to systems is role-based and is removed promptly when someone leaves

- we follow the DfE's [cyber security standards for schools and colleges](#), keep tested offline backups, and patch systems regularly

Retention and disposal

We keep personal data only for as long as it is needed, in line with our retention schedule. The schedule is based on the [Information and Records Management Society \(IRMS\) Toolkit for Schools](#). When records reach the end of their retention period:

- paper is shredded or incinerated, using a certified contractor where needed
- electronic records are permanently deleted, including from backups as they cycle
- devices are securely wiped or destroyed, with a certificate of destruction

Where a record may be needed for a statutory inquiry or legal claim, it is kept under a legal hold until the DPO confirms it can be destroyed.

14. International transfers

We will only transfer personal data outside the UK where it is protected to UK standards. This means transferring it to a country that meets the UK's data protection test (formerly known as adequacy), or using appropriate safeguards such as the ICO's International Data Transfer Agreement or the UK Addendum to the EU standard contractual clauses, supported by a transfer risk assessment.

Many cloud and educational technology services store or access data abroad. Before adopting one, [the DPO / data protection lead] will check where data is held and that a lawful transfer mechanism is in place. Staff must not use services that send personal data overseas without approval.

15. Personal data breaches

Anyone who discovers or suspects a breach must report it to headteacher **immediately**, and in any case on the same day. Do not try to investigate it yourself, and do not delete any evidence.

Typical school breaches include an email or report sent to the wrong parent, a lost laptop or paper file, a safeguarding record left visible, an MIS account compromised by phishing, and a ransomware attack.

The school will:

- contain the breach and recover data where possible
- assess the risk to the people affected
- report it to the ICO **within 72 hours** of becoming aware of it, where it is likely to result in a risk to people's rights and freedoms
- tell the people affected **without undue delay** where the risk to them is high
- record every breach in the breach log, whether or not it is reported, with the facts, effects and action taken
- review what happened and act to stop it happening again

The step-by-step procedure is set out in the appendix.

16. Complaints, training, monitoring and related policies

Data protection complaints

From 19 June 2026, the DUAA requires data controllers to have a process for handling data protection complaints. Anyone who thinks we have misused their personal data can complain to us by [email to the DPO / online form / letter] or in any other way, including in person. We will:

- acknowledge the complaint **within 30 days** of receiving it
- investigate in a way that is reasonable and proportionate to the issue and its impact
- keep the complainant updated and tell them the outcome without undue delay
- keep a record of each complaint and how it was handled

If the complainant is still unhappy, they can complain to the Information Commissioner's Office. [Link to the school's general complaints policy.]

Training

All staff and governors complete data protection training at induction and refresher training at least [annually], with additional training for roles that handle sensitive data. Training records are kept.

Monitoring and review

The DPO monitors compliance with this policy and reports to the governing board at least annually. This policy is reviewed every [two] years, or sooner if the law or guidance changes, and is approved by the governing board.

Related policies

- Privacy notices (pupils, parents, staff, governors, applicants and visitors)
- Records retention schedule
- Child protection and safeguarding policy
- Online safety and acceptable use policies (including AI)
- CCTV policy
- Freedom of information publication scheme
- Complaints policy
- Appropriate policy document (special category data)

Appendix: personal data breach procedure

Every breach is logged; only risky ones go to the ICO

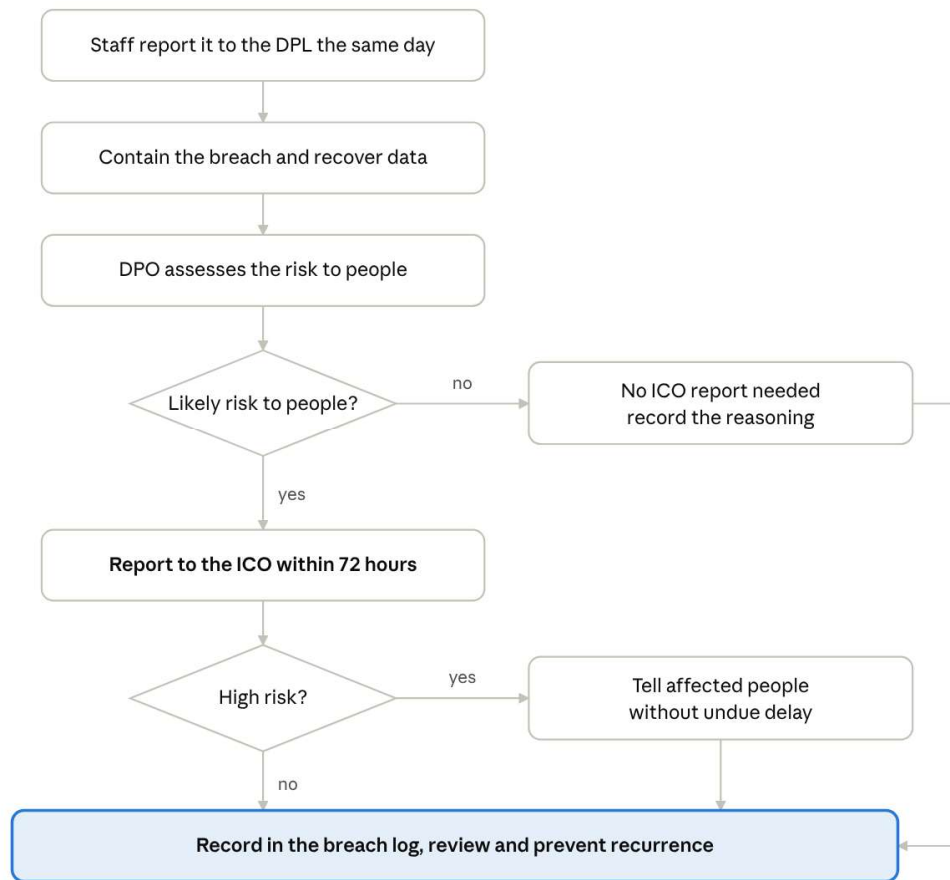


Figure 1: Breach response procedure

Every breach is recorded in the breach log, whatever the risk. The ICO is told only about breaches likely to put people at risk, and the individuals affected are told only when that risk is high.

1. **Report.** The person who finds the breach tells [the data protection lead] immediately, giving what happened, when, what data was involved and whose it was.
2. **Contain.** The data protection lead and DPO act straight away to limit the damage. This may mean recalling a misdirected email or asking the recipient to delete it, disabling compromised accounts, remotely wiping lost devices, and recovering data from backups.
3. **Assess.** The DPO considers the type and sensitivity of the data, how many people are affected, whether it was protected (for example, encrypted), and the likely consequences, such as safeguarding risk, distress, discrimination, fraud or identity theft.
4. **Report to the ICO** within 72 hours of the school becoming aware of the breach, if it is likely to result in a risk to people. Use the [ICO breach reporting service](#). If not all the details are known, report what is known and follow up.
5. **Tell the individuals affected** without undue delay if the risk is high. Use plain language and explain what happened, the likely consequences, what we are doing, what they can do to protect themselves, and how to contact the DPO.

6. **Record and review.** Log every breach, including the facts, effects, decisions and reasons (including why it was not reported, where applicable). The DPO and headteacher review the cause, agree actions such as training or system changes, and report themes to governors.

Where the breach involves possible criminal activity, such as theft or a cyber attack, also inform the police and [Action Fraud / the school's cyber insurer / the DfE and RPA where applicable].