`

Holy Rood Catholic Primary School, Swindon

GDPR Data Protection Policy 2026-2028

`

School Vision:

Belong

At Holy Rood Catholic Primary School, we aim to provide a nurturing and inclusive environment enthused by the Spirit of Christ to enable everyone to make a positive contribution, both to the school and the wider community. We will show love, compassion and respect for others.

A sense of unity will be created by forming relationships that are based on trust, loyalty, forgiveness and acceptance; we will endeavour to act justly and be peacemakers as Christ's disciples, inspired by the Gospel values.

We will encourage a sense of responsibility and help children learn to appreciate God's world around them through reflection, mission, prayer, healing and peace.

Learn

We resolve to develop a sense of awe and wonder at God's creation for our children - where creativity flourishes and everyone is inspired to learn, demonstrating a curiosity about the world around them.

We will strive to ensure that all of our learners are able to face new challenges with confidence, in a Christian learning environment where informed risk taking and a resilient attitude are welcomed, encouraged and achieved.

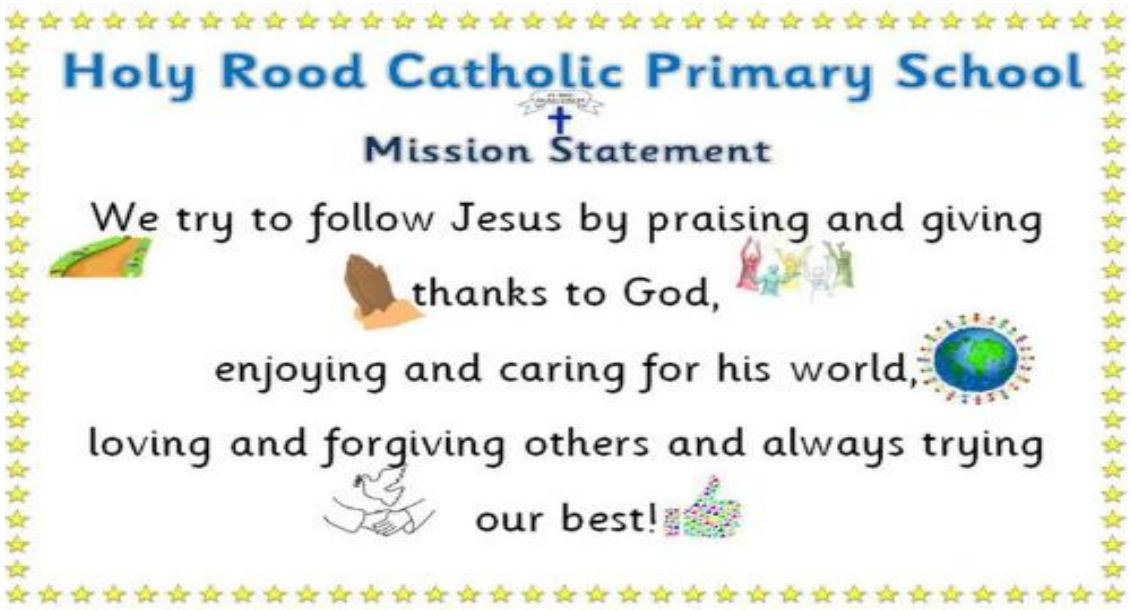
Our positive and enthusiastic approach to teaching and learning will motivate every person. Each will know that they are uniquely loved by God. We will continue to enjoy our learning and reflect on our efforts and achievements, inspiring us to always try our best.

Achieve

The children will be determined in their daily challenges, gaining confidence in their own ability, imagining what they could achieve with continued effort and commitment and working to fulfil the exclusive plan God has for each of them.

By fully engaging in all aspects of school, children will have had the opportunity to go on to become ambitious and competent individuals, always striving to achieve their full potential and positively participating in God's world.

Children's Mission Statement:



`

Contents

`

1. Aims

The school is committed to protecting the privacy and security of personal data and to ensuring that personal data is handled lawfully, fairly and transparently.

The school aims to ensure that all personal data collected, stored, used or otherwise processed by or on behalf of the school is handled in accordance with applicable data protection legislation and the principles set out in this policy.

This includes personal data relating to pupils and former pupils, parents and carers, staff and former staff, applicants, Trustees and Members, volunteers, visitors, contractors, suppliers and other individuals who interact with the School or Trust.

This policy applies to all personal data processed by or on behalf of the school, whether held in electronic, paper or other formats.

The school will take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure.

All staff and others who process personal data on behalf of the school are expected to understand and comply with their responsibilities under this policy and the school's associated data protection procedures.

2. Legislation and Guidance

This policy is designed to support the school's compliance with applicable data protection and privacy legislation, including:

- the **UK General Data Protection Regulation (UK GDPR)**;
- the **Data Protection Act 2018**;
- the **Data (Use and Access) Act 2025**; and
- where applicable, the **Privacy and Electronic Communications Regulations 2003 (PECR)**.

The Data (Use and Access) Act 2025 amended aspects of the UK's data protection and privacy framework. The school will take account of these changes and any associated guidance when reviewing and implementing its data protection procedures.

The policy takes account of guidance published by the **Information Commissioner's Office (ICO)** and the **Department for Education (DfE)** relating to data protection in schools and academies. The school will have regard to relevant ICO guidance and codes of practice when determining how personal data should be collected, used, shared, retained and protected.

The school will also take account of relevant DfE guidance on matters including:

`

- data protection responsibilities and accountability;
- the lawful processing of personal data;
- children's personal data;
- sharing personal data;
- data breaches and information security;
- subject access requests and other individual rights;
- record keeping and retention;
- taking and using photographs and videos;
- CCTV and surveillance;
- filtering and monitoring; and
- the use of generative artificial intelligence and other technology involving personal data.

This policy operates alongside the Trust's funding agreement and Articles of Association and should be read together with the school's related data protection procedures and policies.

The school will review this policy and its associated procedures regularly and when there are significant changes to legislation, regulatory requirements or relevant DfE or ICO guidance.

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 • Genetics • Health – physical or mental

`

	• Sex life or sexual orientation • In Care • Court Orders
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 the school and to Trustees, Members, volunteers, temporary staff, agency workers, contractors and other individuals who process personal data on behalf of the School or Trust, where applicable.

It also applies to external organisations and individuals who process personal data on behalf of the Trust or School. Such organisations and individuals must comply with applicable data protection requirements and any contractual or other obligations relating to the processing and protection of personal data.

`

All individuals within the scope of this policy are responsible for ensuring that personal data is handled securely, lawfully and in accordance with this policy and the school's data protection procedures.

Failure by a member of staff to comply with this policy may result in appropriate action being taken under the school's disciplinary procedures. The action taken will depend on the nature and circumstances of the breach.

Where an external organisation or individual fails to comply with applicable data protection requirements or contractual obligations, the School or Trust may take appropriate action in accordance with the relevant contract or other arrangements.

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Trust has appropriate arrangements in place to comply with applicable data protection legislation and to protect personal data processed by or on behalf of the School and Trust.

The Board of Trustees will provide appropriate oversight of data protection arrangements and ensure that sufficient policies, procedures, resources and accountability arrangements are in place to support compliance with data protection requirements.

5.2 Data protection officer

The Trust has appointed a Data Protection Officer (DPO) in accordance with applicable data protection legislation.

The DPO will:

- advise the Trust, the School, the Board of Trustees and staff on their obligations under applicable data protection legislation;
- monitor compliance with data protection legislation, this policy and the Trust's data protection policies and procedures;
- provide advice and guidance on data protection impact assessments and monitor their implementation where appropriate;
- cooperate with and act as the contact point for the Information Commissioner's Office (ICO);
- act as a contact point for individuals in relation to the processing of their personal data and the exercise of their data protection rights;
- provide advice and recommendations on data protection matters to the Trust, School and Board of Trustees;
- raise significant data protection risks or concerns with the appropriate senior leaders or Board of Trustees; and
- undertake or support other activities required of the DPO under applicable data protection legislation.

`

The DPO will have an appropriate level of independence when carrying out their duties and will not determine the purposes or means of processing personal data on behalf of the Trust. The Trust will ensure that the DPO is involved, properly and in a timely manner, in all issues relating to the protection of personal data.

The DPO is the primary point of contact for the ICO in relation to data protection matters and will cooperate with the ICO as required..

Data Protection Officer contact details:

Email: DPOadmin@holyroodprimary.co.uk

The Trust will ensure that current DPO contact details are made available to individuals through the school's privacy notices and other appropriate communications.

5.3 Headteacher

The Headteacher is responsible for supporting the day-to-day implementation of the Trust's data protection arrangements within the school.

The Headteacher will ensure that staff are aware of their responsibilities under this policy and that appropriate procedures are followed when personal data is collected, used, shared, stored or otherwise processed.

The Headteacher will work with the Data Protection Officer and other relevant staff to address data protection issues, manage risks and respond appropriately to data protection incidents and concerns.

The Headteacher will escalate significant data protection risks, breaches or compliance concerns to the appropriate senior leaders, the Data Protection Officer and, where appropriate, the Board of Trustees.

5.4 All staff

All staff are responsible for ensuring that personal data is processed in accordance with this policy, the Trust's data protection procedures and applicable data protection legislation.

Staff are responsible for:

- collecting, using, storing, sharing and otherwise processing personal data lawfully, fairly and securely;
- only accessing and using personal data where they have an appropriate work-related need to do so;
- keeping personal data accurate and up to date where appropriate;
- informing the school of changes to their own personal details, such as a change of address or contact details;

`

- keeping personal data secure and following the school's information security procedures;
- maintaining confidentiality and not disclosing personal data to unauthorised individuals or organisations; and
- completing any required data protection training.

Staff must contact the DPO for advice:

- if they have any questions about the operation of this policy or their responsibilities under data protection legislation;
- if they have concerns that this policy or data protection requirements are not being followed;
- if they are unsure whether there is a lawful basis for processing personal data in a particular circumstance;
- before relying on consent as the lawful basis for processing, where appropriate;
- when preparing or reviewing a privacy notice;
- when responding to, or receiving, a request to exercise an individual's data protection rights;
- before transferring personal data outside the UK, where applicable;
- immediately if they become aware of, suspect or believe that a personal data breach may have occurred;
- before starting a new activity, system, project or process that may have a significant impact on individuals' privacy or involve the processing of personal data in a new or substantially different way;
- where a Data Protection Impact Assessment (DPIA) may be required;
- when entering into arrangements involving the processing or sharing of personal data with third parties;
- when developing or reviewing contracts that involve the processing of personal data; and
- where they are unsure about any other data protection requirement or risk.

Staff should report a suspected personal data breach as soon as possible and should not delay reporting while attempting to establish whether the incident meets the legal definition of a personal data breach.

Staff must not attempt to conceal, delete or alter evidence relating to a suspected data breach or other data protection incident.

All staff are expected to cooperate with the DPO and the Trust when responding to data protection requests, incidents, investigations or other compliance matters.

6. Data protection principles

The UK GDPR sets out a number of data protection principles that the Trust must comply with when processing personal data.

Personal data must be:

`

- **Processed lawfully, fairly and transparently** in relation to the individual.
- **Collected for specified, explicit and legitimate purposes** and not further processed in a way that is incompatible with those purposes.
- **Adequate, relevant and limited to what is necessary** in relation to the purposes for which it is processed.
- **Accurate and, where necessary, kept up to date**, with reasonable steps taken to correct or delete inaccurate personal data without undue delay.
- **Kept for no longer than is necessary** for the purposes for which it is processed, subject to any legal, regulatory or legitimate requirements to retain it for longer.
- **Processed securely**, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, damage or alteration.
- **Processed in accordance with the accountability principle**, meaning that the Trust must be able to demonstrate compliance with the data protection principles and maintain appropriate records, policies, procedures and other measures to support this.

These principles apply to all personal data processed by or on behalf of the Trust, regardless of the format in which it is held.

The School and Trust will take appropriate measures to demonstrate compliance with these principles and will provide staff with appropriate guidance and training to support their responsibilities.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

The Trust will only process personal data where there is a valid lawful basis under applicable data protection legislation. The appropriate lawful basis must be identified for each processing activity and, where required, documented.

The lawful bases available under the UK GDPR are:

- **Consent** – the individual has given clear, specific, informed and freely given consent to the processing of their personal data for one or more specific purposes.
- **Contract** – the processing is necessary for a contract with the individual, or because the individual has asked the Trust to take specific steps before entering into a contract.
- **Legal obligation** – the processing is necessary for the Trust to comply with a legal obligation.
- **Vital interests** – the processing is necessary to protect someone's life.
- **Public task** – the processing is necessary for the Trust to perform a task in the public interest or in the exercise of official authority, where the task or function has a clear basis in law.

`

- **Recognised legitimate interests** – where applicable, the processing is necessary for one of the recognised legitimate interests specified in data protection legislation, subject to the conditions and restrictions that apply.
- **Legitimate interests** – the processing is necessary for the legitimate interests of the Trust or a third party, except where those interests are overridden by the individual's interests or fundamental rights and freedoms. This lawful basis is subject to additional restrictions where an organisation is acting as a public authority in the performance of its official tasks.

The Trust will determine the most appropriate lawful basis for each processing activity and will ensure that the chosen basis is appropriate to the purpose and circumstances of the processing.

Where the Trust relies on **consent**, consent must be freely given, specific, informed and unambiguous. The Trust will keep appropriate records of consent and will provide individuals with a genuine opportunity to withdraw consent where applicable. Consent will not be used where there is no genuine choice or where another lawful basis is more appropriate.

Where personal data relates to children, the Trust will take particular care to protect their interests and will consider their age, understanding and circumstances when determining how their personal data is processed.

Where the Trust offers an **information society service directly to a child** and relies on consent as the lawful basis, the additional requirements relating to children's consent will be followed. Where the child is under 13, consent must be provided or authorised by a person with parental responsibility, and reasonable efforts must be made to verify that consent. These requirements do not apply where the service is a preventive or counselling service. Where appropriate, the Trust may instead rely on another lawful basis.

Special category data

Where the Trust processes **special category personal data**, it must identify both:

- a lawful basis under Article 6 of the UK GDPR; and
- an appropriate condition for processing under Article 9 of the UK GDPR and, where applicable, the Data Protection Act 2018.

Where required, the Trust will also identify and document any additional requirements or safeguards that apply to the processing of special category data.

Transparency

The Trust will process personal data fairly and transparently. When personal data is collected directly from an individual, the Trust will provide the individual with the information required by data protection legislation through an appropriate privacy notice or other privacy information.

`

Privacy information will explain, as appropriate, the purposes for which personal data is processed, the lawful basis relied upon, relevant information about recipients or sharing, retention periods, individuals' rights and other information required by law.

The Trust will keep its privacy notices under review and update them when there are significant changes to the purposes, lawful basis or methods of processing personal data.

7.2 Limitation, minimisation and accuracy

The Trust will only collect and process personal data for specified, explicit and legitimate purposes. Individuals will be provided with appropriate information about the purposes for which their personal data is collected and used through the school's privacy notices and other relevant privacy information.

Personal data will only be collected and processed to the extent that it is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

Staff must only access and process personal data where they have an appropriate work-related need to do so. Staff must not collect, access, use or retain personal data simply because it may be useful in the future.

Where the Trust intends to use personal data for a new purpose that is not compatible with the original purpose, the Trust will assess whether the proposed processing is lawful and whether individuals need to be provided with additional information before the processing takes place. Consent will only be sought where consent is the appropriate lawful basis; it will not be used as a substitute for another lawful basis.

The Trust will take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date. Staff should report inaccurate or outdated personal data to the appropriate member of staff or the DPO so that it can be corrected without undue delay.

Where an individual, parent or carer notifies the school that personal data is inaccurate, the school will take appropriate steps to verify and correct the information where necessary.

Personal data will not be retained for longer than is necessary for the purpose for which it is processed, unless there is a legal, regulatory, safeguarding, financial, operational or other legitimate requirement to retain it for longer.

When personal data is no longer required, it will be securely deleted, destroyed or anonymised in accordance with the Trust's records retention and disposal arrangements. Paper records containing personal data must be disposed of securely, for example through confidential waste arrangements, where appropriate.

`

Staff must not independently delete or destroy records where they are subject to a retention requirement, legal hold, investigation, safeguarding matter, audit requirement or other reason for continued retention. Where there is any uncertainty about whether information can be deleted or destroyed, staff should seek advice from the appropriate member of staff or the DPO.

The school will maintain and apply appropriate retention and disposal arrangements to support the secure and consistent management of personal data.

8. Data Sharing

The Trust will only share personal data where there is a lawful basis for doing so and where the sharing is fair, necessary, proportionate and secure.

Before sharing personal data, the school will consider:

- the purpose for which the information is being shared;
- the lawful basis for the sharing;
- what information is necessary and proportionate to share;
- who needs to receive the information and what they will use it for;
- whether the individual needs to be informed about the sharing;
- whether any additional safeguards are required, particularly where children or special category data are involved; and
- how the information will be shared securely.

The school will not normally share more personal data than is necessary for the particular purpose.

Safeguarding and emergencies

Personal data may be shared with other schools, children's social care, local authorities, health services, the police, emergency services or other appropriate organisations where this is necessary to safeguard a child or adult, protect someone's health or safety, or respond to an emergency.

Consent will not normally be required where information needs to be shared for safeguarding purposes and there is another appropriate lawful basis for doing so. Staff must not delay necessary safeguarding action while seeking consent where doing so could place a child or another individual at risk.

The Designated Safeguarding Lead or another appropriately authorised member of staff will determine whether safeguarding information needs to be shared and will ensure that appropriate records are maintained of significant information-sharing decisions.

Personal data may also be shared where necessary to protect staff from a significant risk to their safety or to support the appropriate management of incidents involving pupils, parents, carers or other individuals.

`

Sharing with other organisations

The school may share personal data with other schools, local authorities, government departments, public authorities, health services, professional advisers and other organisations where there is a lawful basis and the sharing is necessary and appropriate.

Where information is shared routinely, the school will consider whether a data sharing agreement or other appropriate documented arrangement is required.

Where personal data is shared with law enforcement or government bodies, the school will comply with any applicable legal requirements and will only disclose information that is lawful and necessary for the relevant purpose. This may include, where applicable:

- the prevention or detection of crime or fraud;
- the investigation or prosecution of offences;
- the assessment or collection of taxes or duties;
- legal proceedings or the establishment, exercise or defence of legal claims;
- statutory or regulatory functions; and
- safeguarding and the protection of individuals from harm.

The school will not assume that consent is required for every disclosure. The appropriate lawful basis and any other legal requirements will be considered for each disclosure.

Suppliers, contractors and other processors

Where a supplier, contractor or other organisation processes personal data on behalf of the Trust, the organisation will be treated as a **processor** where applicable under data protection legislation.

The Trust will only appoint processors that provide sufficient guarantees that they will implement appropriate technical and organisational measures to meet applicable data protection requirements.

Where required, the Trust will have a written contract or other legally binding arrangement with the processor setting out the required data protection obligations, including requirements relating to confidentiality, security, sub-processors, assistance with individuals' rights, personal data breaches, audits and the deletion or return of personal data.

The school will only provide a processor with the personal data that is necessary for it to provide the agreed service.

Where an organisation is receiving personal data for its own purposes rather than processing it solely on behalf of the Trust, the appropriate controller or other legal relationship will be established and the relevant data protection requirements will be followed.

`

Data sharing for research and statistical purposes

Personal data may be shared for research, statistical or other purposes where there is a lawful basis for doing so and all applicable data protection requirements are met.

Where possible, information will be anonymised or appropriately pseudonymised before it is shared. Where personal data must be shared, appropriate safeguards will be considered and applied.

International transfers

The Trust will not transfer personal data to, or make personal data accessible to, organisations outside the UK unless the transfer is permitted under applicable data protection legislation.

Where an international transfer is a restricted transfer, the Trust will ensure that the transfer is covered by an applicable UK adequacy regulation, appropriate safeguards or a relevant exception under data protection legislation.

Staff must seek advice from the DPO before arranging a new international transfer of personal data or using a service that involves personal data being transferred to, or accessed by, an organisation outside the UK.

Secure sharing

Personal data must be shared securely and only through approved methods and systems. Staff must check that information is being sent to the correct recipient and that the amount of information shared is appropriate for the purpose.

Any accidental or unauthorised disclosure of personal data must be reported immediately in accordance with the school's personal data breach procedures.

8.1 CPOMS and Safeguarding Records

Where a pupil transfers to another school or educational setting, including during the academic year, at the end of an academic year or at the end of a key stage, the school will transfer relevant safeguarding and child protection records to the pupil's new setting in accordance with applicable safeguarding and data protection requirements.

Where the school uses CPOMS to maintain safeguarding records, records will normally be transferred securely to the receiving school using the available electronic transfer functionality. Where electronic transfer is not available or appropriate, the school may provide the records in another secure format, such as a password-protected or otherwise appropriately secured electronic document.

`

Only safeguarding and child protection information that is relevant and appropriate to the receiving setting will be transferred. The school will ensure that information is shared securely and with an appropriately authorised recipient.

Following a pupil's transfer, the school will retain copies of safeguarding and child protection records where required by applicable legislation, statutory guidance or the School's records retention arrangements. Records will be securely archived or otherwise restricted from routine access where appropriate.

Access to archived safeguarding records will be limited to authorised staff with a legitimate work-related need to access them. Archived records will not be retained indefinitely. They will be securely deleted or destroyed when the applicable retention period has expired, subject to any legal, safeguarding, regulatory or other requirement to retain them for longer.

The school will maintain appropriate retention and disposal arrangements for safeguarding records held in CPOMS and will review these arrangements when CPOMS introduces new functionality or when applicable statutory guidance, legal requirements or the school's retention requirements change.

Staff must not manually delete, alter or destroy safeguarding records outside the school's approved retention and disposal arrangements. Any uncertainty about the retention, transfer or deletion of safeguarding records should be referred to the Designated Safeguarding Lead and, where appropriate, the Data Protection Officer.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to obtain access to the personal data that the Trust holds about them. This is known as a Subject Access Request (SAR)**.**

A SAR may be made verbally or in writing and does not need to use the words "subject access request" or refer specifically to the UK GDPR. Requests may be made by letter, email, telephone, in person or through other appropriate communication channels.

A SAR may include a request for:

- confirmation that the individual's personal data is being processed;
- access to a copy of their personal data;
- the purposes for which their personal data is being processed;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom personal data has been or will be disclosed;
- the period for which the personal data is expected to be retained, or the criteria used to determine that period;
- information about the source of the personal data where it was not collected from the individual;

`

- information about automated decision-making, where applicable, including the relevant information required by data protection legislation; and
- other supplementary information required under applicable data protection legislation.

The Trust will respond to a valid SAR without undue delay and normally within one calendar month of receiving it. In certain circumstances, the response period may be extended by up to a further two calendar months where the request is complex or the individual has made a number of requests. Where an extension is required, the individual will be informed within the initial one-month period and given the reasons for the extension.

The Trust may request appropriate information to confirm the identity of the requester where this is reasonably necessary. The Trust may also seek reasonable clarification about the information requested where this is necessary to identify the information being sought. Requests for identification or clarification will be proportionate and will not be used unnecessarily to delay a response.

The Trust will make reasonable and proportionate searches for personal data falling within the scope of a SAR and will take appropriate steps to ensure that information is provided securely.

Personal data relating to other individuals may be subject to appropriate restrictions or redaction where disclosure would adversely affect the rights and freedoms of those individuals or where another exemption applies.

The Trust will not normally charge a fee for responding to a SAR. A reasonable fee may be charged, or a request may be refused, where permitted by data protection legislation, including where a request is manifestly unfounded or excessive. Any decision to refuse a request or charge a fee will be made on its individual circumstances and will be appropriately documented.

Where a SAR is refused in whole or in part, the Trust will explain the reasons for the decision unless applicable law prevents it and will inform the requester of their right to complain to the Information Commissioner's Office (ICO) and to seek a judicial remedy where applicable.

Staff responsibilities

All staff must recognise that a request for personal information may constitute a SAR, even where the individual does not use the term "subject access request".

If a member of staff receives or becomes aware of a request for access to personal data, they must forward or report it to the DPO as soon as possible and should not attempt to deal with the request themselves unless they have been authorised to do so.

`

Staff must not delete, amend, conceal or otherwise alter records because a SAR has been received. They must cooperate with the DPO and provide access to relevant records when requested.

The DPO will coordinate the Trust's response to SARs and will ensure that requests are handled in accordance with applicable data protection legislation and the Trust's data protection procedures.

9.2 Children and subject access requests

Personal data relating to a child belongs to the child. A parent or carer does not automatically have a right to access their child's personal data simply because they have parental responsibility.

A parent or carer may make a subject access request on behalf of a child where the child has authorised them to do so or where it is appropriate for the parent or carer to exercise the child's right on their behalf.

There is no fixed age at which a child is automatically considered competent to exercise their data protection rights. The Trust will consider the child's level of maturity and understanding on a case-by-case basis, taking account of the child's ability to understand:

- what a subject access request is;
- what information is being requested;
- what the consequences of providing or withholding the information may be; and
- whether they wish their personal data to be disclosed to the person making the request.

Where a child is considered sufficiently mature and understands the implications of the request, the Trust will normally expect the child to exercise their own right of access or to provide their consent before information is disclosed to a parent or carer.

Where a child is not considered sufficiently mature to exercise their right of access independently, the Trust may allow a person with parental responsibility to exercise the child's right on their behalf where this is appropriate and, in the child’s, best interests.

The Trust will consider each request individually and will take into account the child's wishes and interests. The fact that a person has parental responsibility does not, by itself, mean that information must be disclosed to them.

Where there are concerns that disclosure to a parent or carer may not be in the child's best interests, or where there are safeguarding concerns, the Trust will seek advice from the Data Protection Officer and, where appropriate, the Designated Safeguarding Lead before responding.

`

The Trust may also withhold or redact information where disclosure would adversely affect the rights and freedoms of another individual or where another exemption under data protection legislation applies.

All requests for access to a child's personal data made by a parent, carer or other person on the child's behalf must be referred to the DPO for consideration where there is any uncertainty about the child's competence, consent, best interests or the information that can be disclosed.

9.3 Responding to subject access requests

When responding to a Subject Access Request (SAR), the Trust will:

- take reasonable and proportionate steps to verify the identity of the requester where necessary;
- where appropriate, verify that a person making a request on behalf of another individual has the necessary authority to do so;
- respond without undue delay and normally within **one calendar month** of receiving the request;
- provide the information free of charge in most circumstances;
- make a reasonable and proportionate search for the personal data covered by the request;
- provide information in a clear and accessible form and take appropriate steps to provide it securely; and
- where the request is complex or the individual has made a number of requests, extend the response period by up to a further **two calendar months**, where permitted by data protection legislation.

Where an extension is required, the Trust will inform the requester within the first calendar month and explain why the extension is necessary. The Trust will respond as soon as possible and will not treat a request as complex simply because it involves a large amount of information or requires information to be retrieved or redacted. (gov.uk)

Where the Trust reasonably requires clarification of a request, it may ask the requester to clarify the information they are seeking. The Trust will not require a requester to narrow their request, but reasonable clarification may help the Trust identify and locate the relevant information.

Information that may be withheld or restricted

The right of access is subject to exemptions and restrictions under data protection legislation. The Trust may withhold or redact information where an applicable exemption or restriction applies.

This may include, where the relevant legal requirements are met:

- information about another individual where disclosure would adversely affect that person's rights and freedoms;

`

- information relating to child abuse where the relevant statutory exemption applies;
- certain health, education or social work information;
- information subject to legal professional privilege;
- certain information relating to crime and taxation;
- information contained in confidential references;
- certain information relating to legal proceedings, examinations or research; and
- information where disclosure would otherwise be restricted or prohibited by law.

The Trust will consider any applicable exemption on the individual circumstances of the request. Exemptions will not be applied automatically and the DPO will be consulted where an exemption may apply. (ico.org.uk)

Manifestly unfounded or excessive requests

The Trust may refuse to comply with a SAR, or may charge a reasonable fee, where the request is manifestly unfounded or excessive, as permitted by data protection legislation.

Each request will be considered on its individual circumstances. A request will not automatically be treated as manifestly unfounded or excessive simply because the individual has made a previous request, has made repeated requests, or has requested a large amount of information. The Trust will maintain evidence supporting any decision to refuse a request or charge a fee. (ico.org.uk)

Where a reasonable fee is charged, it will be based on the permitted administrative costs and the Trust will explain the reason for the fee to the requester.

Refusing a request

If the Trust refuses a SAR, in whole or in part, it will inform the requester within the applicable response period and explain the reasons for the decision, unless applicable law prevents the Trust from doing so.

The requester will also be informed of their right to complain to the Trust, to raise a concern with the Information Commissioner's Office (ICO), and to seek a judicial remedy where applicable. (ico.org.uk)

The DPO will coordinate responses to SARs and will ensure that decisions to withhold information, apply an exemption, extend the response period or charge a fee are appropriately considered and documented.

9.4 Other data protection rights of the individual

In addition to the right to make a Subject Access Request and to receive appropriate privacy information, individuals have a range of rights under data protection

`

legislation. The rights available to an individual will depend on the circumstances and the lawful basis being relied upon for the processing.

These rights may include:

- **The right to withdraw consent** – where processing is based on consent, an individual may withdraw their consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before consent was withdrawn.
- **The right to rectification** – an individual may ask for inaccurate personal data to be corrected or incomplete personal data to be completed.
- **The right to erasure** – in certain circumstances, an individual may ask for their personal data to be erased.
- **The right to restriction of processing** – in certain circumstances, an individual may ask the Trust to restrict the processing of their personal data.
- **The right to object** – in certain circumstances, an individual may object to the processing of their personal data, including processing based on legitimate interests or the performance of a task in the public interest or in the exercise of official authority.
- **Rights relating to direct marketing** – individuals have an absolute right to object to the processing of their personal data for direct marketing purposes.
- **Rights relating to automated decision-making and profiling** – individuals have rights in relation to certain decisions based solely on automated processing, including where those decisions produce legal effects or similarly significant effects.
- **The right to data portability** – in certain circumstances, an individual may request their personal data in a structured, commonly used and machine-readable format and may ask for it to be transmitted to another organisation.
- **The right to complain** – individuals may raise concerns about the Trust's handling of their personal data and may complain to the Information Commissioner's Office (ICO).

Some of these rights are subject to specific conditions, exemptions or restrictions. The Trust will assess each request according to the circumstances, the lawful basis for processing and the applicable requirements of data protection legislation.

The right to erasure, restriction and objection does not apply in all circumstances. In particular, these rights may be limited where the Trust has a legal obligation to retain or process information, or where another lawful basis or exemption applies.

Where an individual exercises a data protection right, the Trust will respond without undue delay and within the applicable statutory timeframe. Where permitted, the Trust may extend the response period where a request is complex or the individual has made a number of requests.

The Trust may request proportionate information to verify the identity of an individual where this is reasonably necessary before responding to a request.

`

Individuals should normally submit requests to exercise their data protection rights to the Data Protection Officer (DPO). However, requests do not have to use a particular form or wording.

All staff must recognise that a request relating to an individual's personal data may constitute an exercise of a data protection right, even if the individual does not refer to a specific legal right. Staff who receive such a request must forward or report it to the DPO as soon as possible and must not attempt to deal with the request themselves unless authorised to do so.

The DPO will coordinate responses to requests and will ensure that the Trust's decisions and any applicable exemptions or restrictions are appropriately considered and documented.

10. Parental requests to see the educational record

Parents or others with parental responsibility may ask the school for access to information held about their child, including the child's educational record.

For an academy, the specific statutory right of parents to access a pupil's educational record under the Education (Pupil Information) (England) Regulations 2005 does not apply. The school is therefore not subject to the 15-school-day access requirement under those Regulations.

However, parents and others with parental responsibility may have rights to access their child's personal data under data protection legislation. Where a request seeks personal data about the child, the request may constitute a Subject Access Request (SAR) and will be handled in accordance with sections 9.1 to 9.4 of this policy.

A parent or person with parental responsibility does not automatically have an unrestricted right to access all information relating to their child. The school will consider the child's age, maturity and understanding, the nature of the information requested, the child's wishes and interests, any safeguarding concerns and the rights and freedoms of other individuals when deciding whether information can be disclosed.

Requests should normally be directed to the Data Protection Officer (DPO). However, requests do not need to be made in a particular format. Staff who receive a request for information about a pupil must refer it to the DPO as soon as possible where it may involve the exercise of a data protection right.

The school will respond to requests within the applicable statutory timeframe where the request constitutes a data protection request. Where the School receives a request that falls outside the statutory data protection rights, it will consider the request on a case-by-case basis and will respond within a reasonable period.

The school will not disclose information where, doing so would be unlawful, would adversely affect the rights and freedoms of another individual, would conflict with a

`

relevant exemption or restriction, or would not be in the child's best interests where this is relevant to the decision.

This section should be read alongside the School's Procedures for Subject Access Requests and the provisions of sections 9.1 to 9.4 of this policy.

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 the Head Teacher.

12. Telephone Recording

We record all incoming and outgoing telephone calls to protect the interests of one or more participants. All incoming callers are advised that the call is recorded. We do not need to ask individuals' permission to record calls. All recordings are retained for one month and the data is then deleted.

13. 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.

`

14. 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 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)
- All new systems and suppliers, including 3rd party suppliers will be reviewed in line with regulatory needs, including Due Diligence, DPIA (Data Protection Impact Assessment) as necessary
- 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

`

15. 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 ICT Policy/Acceptable Use Agreement)
- 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)

16. 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. Holy Rood Catholic Primary school refers to the *Information and Records Management Society toolkit for schools* guidelines.

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.

17. 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

18. Training

The school will provide appropriate data protection training to staff and other individuals who process personal data on behalf of the School or Trust as part of their induction and, where appropriate, on an ongoing basis.

Training will be proportionate to an individual's role and responsibilities and will cover the key data protection and information security requirements relevant to their work.

The school will provide additional or refresher training where necessary, including where there are significant changes to data protection legislation, regulatory requirements, ICO or DfE guidance, School or Trust procedures, systems or working practices.

Trustees and Members will be provided with appropriate information or training to support their understanding of their data protection responsibilities and governance responsibilities where relevant.

Staff and other individuals who are required to complete data protection training are expected to do so within the timescales set by the School or Trust.

The school will maintain appropriate records of completed data protection training.

19. Monitoring arrangements

The Data Protection Officer (DPO) will monitor the implementation of this policy and provide advice and recommendations to the Trust on its effectiveness and any changes that may be required.

The Trust will review this policy every 2 years or whenever there are significant changes to data protection legislation, regulatory requirements, ICO or DfE guidance, the school's processing activities, systems or procedures.

The review will consider, where appropriate:

`

- changes to applicable legislation and regulatory guidance;
- significant data protection risks or incidents;
- findings from audits, monitoring or compliance reviews;
- changes to the School's or Trust's processing activities and systems;
- feedback from staff and individuals; and
- lessons learned from data protection incidents or complaints.

Any significant amendments to the policy will be approved in accordance with the Trust's governance arrangements.

The Board of Trustees will receive appropriate assurance about the Trust's data protection arrangements and significant changes to this policy.

20. Links with other policies

This data protection policy is linked to our:

- Safeguarding Policy
- E Safety
- Privacy Notice for Parents and Carers
- Privacy Notice for Staff
- Subject Access Request Procedures
- Privacy Notice for Governors and other Visitors

`

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 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. (Actions relevant to specific data types are set out at the end of this procedure)
- 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 on the school's 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

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. This is not an exhaustive list but sets out some of the processes and procedures that will be adopted where necessary.

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 it is removed
- 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