Holy Trinity
CE Primary Academy

Great Cheverell
Devizes
SN10 5TL
01380 813 796
www.holy-trinity.co.uk

Data Protection Policy

Vision Statement
At Holy Trinity CE Primary Academy, inspired by and rooted in Christian values and teaching, we nurture children to become aspirational, courageous, compassionate, and joyful young people.

The values of our school: Courage, Joy, Aspiration, and Compassion

Status	**Statutory**
Author	**J. Shatford DPO**
Approval Date and by	**November 2022**
Review Frequency	**As required but no less frequently than two years**
Last Review	**November 2021**
Review Due	**November 2022**
Committee	**Sub committee**

Contents

1 Policy Statement

1.1 Everyone has rights about the way in which their personal data is handled. During our activities at Holy Trinity CE Primary Academy -we will collect, store and process personal data about our pupils, workforce, parents, and others. This makes us a data controller in relation to that personal data and therefore required to register our processing activities with the Information Commissioners Office (ICO).

1.2 We are committed to the protection of all personal data and special category personal data for which we are the data controller.

1.3 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines and or compensation payments being applied.

1.4 All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

2 About this policy

2.1 The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the UK-General Data Protection Regulation ('UK-GDPR'), the Data Protection Act 2018 (DPA), and other regulations (together 'Data Protection Legislation').

2.2 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

3 Definition of data protection terms

3.1 A list of definitions is included in the Annex to this policy.

4 Data Protection Officer

1.1 As a public authority we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Mr Jeremy Shatford who may be contacted in writing to the school clearly labelled "Data Protection", or by email to dpo@jeremyshatford.co.uk.

4.1 The DPO is responsible for monitoring and facilitating compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.2 The DPO is also the central point of contact for data subjects, the Information Commissioners Office (ICO), and others in relation to matters of data protection.

5 Data protection principles

5.1 Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

- 5.1.1 Processed fairly and lawfully and transparently in relation to the data subject.
- 5.1.2 Processed for specified, lawful purposes and in a way which is not incompatible with those purposes.
- 5.1.3 Adequate, relevant, and not excessive for the purpose.
- 5.1.4 Accurate and up to date.
- 5.1.5 Not kept for any longer than is necessary for the purpose, and
- 5.1.6 Processed securely using appropriate technical and organisational measures.

5.2 Personal Data must also:

5.2.1 Be processed in line with data subjects' rights.

5.2.2 Not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any processing of personal data by the Academy.

6 Fair and lawful processing

6.1 Data Protection Legislation does not prevent the processing of personal data but ensures that it is done fairly and without adversely affecting the rights of the data subject.

6.2 For personal data to be processed fairly, data subjects must be told:

6.2.1 That the personal data is being processed.

6.2.2 Why the personal data is being processed.

6.2.3 What the lawful basis is for that processing (see below).

6.2.4 Whether the personal data will be shared, and if so with whom.

6.2.5 The period for which the personal data will be held.

6.2.6 The existence of the data subject's rights in relation to the processing of that personal data, and

6.2.7 The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

6.3 We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any processing.

6.4 For personal data to be processed lawfully, it must be processed based on one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

6.4.1 Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract.

6.4.2 Where the processing is necessary to comply with a legal obligation that we are subject to, (e.g., the Education Act 2011).

6.4.3 Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest; and

6.4.4 Where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

6.5 When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

6.5.1 Where the processing is necessary for employment law purposes, for example in relation to sickness absence.

6.5.2 Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment.

6.5.3 Where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities, and

6.5.4 Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

6.6 We will inform data subjects of the above by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter unless we have already provided this information such as at the time when a pupil joins us.

6.7 If any data user is in doubt as to whether they can use any personal data for any purpose, then they must contact the DPO before doing so.

7 Vital Interests

7.1 There may be circumstances where it is considered necessary to process personal data or special category personal data to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not able to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although often this will be retrospective.

8 Consent

8.1 Where none of the other bases for processing set out above apply then the school must seek the consent of the data subject before processing any personal data for any purpose.

8.2 There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

8.3 When pupils and or our Workforce join the academy a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

8.4 In relation to all pupils under the age of [12/13] years old we will seek consent from an individual that has the parental responsibility for that pupil.

8.5 If consent is required for any other processing of personal data of any data subject, then the form of this consent must:

- 8.5.1 Inform the data subject of exactly what we intend to do with their personal data.
- 8.5.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- 8.5.3 Inform the data subject of how they can withdraw their consent.

8.6 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

8.7 The DPO must always be consulted in relation to any consent form before consent is obtained.

8.8 A record must always be kept of any consent, including how it was obtained and when.

9 Processing for limited purposes

9.1 During our activities, we may collect and process the personal data set out in our Schedule of Processing Activities (or data mapping). This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other schools, parents, other pupils, or members of our workforce).

9.2 We will only process personal data for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

10 Notifying data subjects

10.1 If we collect personal data directly from data subjects, we will inform them about:

- 10.1.1 Our identity and contact details as data controller and those of the DPO.
- 10.1.2 The purpose or purposes and legal basis for which we intend to process that personal data.
- 10.1.3 The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- 10.1.4 Whether the personal data will be transferred outside the European Economic Area ('EEA') and if so the safeguards in place.
- 10.1.5 The period for which their personal data will be stored, by reference to our Retention and Destruction Policy.

10.1.6 The existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and

10.1.7 The rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

10.2 Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible, thereafter, informing them of where the personal data was obtained from.

11 Adequate, relevant, and non-excessive processing

11.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by Data Protection Legislation.

12 Accurate data

12.1 We will ensure that personal data we hold is accurate and kept up to date.

12.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

12.3 Data subjects have a right to have any inaccurate personal data rectified. See further below in relation to the exercise of this right.

13 Timely processing

13.1 We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.

14 Processing in line with data subject's rights

14.1 We will process all personal data in line with data subjects' rights, their right to:

14.1.1 Request access to any personal data we hold about them.

14.1.2 Object to the processing of their personal data, including the right to object to direct marketing.

14.1.3 Have inaccurate or incomplete personal data about them rectified.

14.1.4 Restrict processing of their personal data.

14.1.5 Have personal data we hold about them erased.

14.1.6 Have their personal data transferred, and

14.1.7 Object to the making of decisions about them by automated means.

15 The Right of Access to Personal Data

15.1 Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure. A copy of which is available on the school website or on request from the academy office.

16 The Right to Object

16.1 In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking based on a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

16.2 An objection to processing does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the data subject.

16.3 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

16.4 In respect of direct marketing any objection to processing must be complied with.

16.5 The academy is not obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

17 The Right to Rectification

17.1 If a data subject informs the academy that personal data held about them by the academy is inaccurate or incomplete, then we will consider that request and provide a response within one month.

17.2 If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case.

17.3 We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

18 The Right to Restrict Processing

18.1 Data subjects have a right to "block" or suppress the processing of personal data. This means that the academy can continue to hold the personal data but not do anything else with it.

18.2 The academy must restrict the processing of personal data:

18.2.1 Where it is in the process of considering a request for personal data to be rectified (see above).

18.2.2 Where the academy is in the process of considering an objection to processing by a data subject.

18.2.3 Where the processing is unlawful, but the data subject has asked the academy not to delete the personal data, and

18.2.4 Where the academy no longer needs the personal data, but the data subject has asked the academy not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the academy.

18.3 If the academy has shared the relevant personal data with any other organisation, then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

18.4 The DPO must be consulted in relation to requests under this right.

19 The Right to Be Forgotten

19.1 Data subjects have a right to have personal data about them held by the academy erased only in the following circumstances:

19.1.1 Where the personal data is no longer necessary for the purpose for which it was collected.

19.1.2 When a data subject withdraws consent – which will apply only where the Academy is relying on the individuals consent to the processing.

19.1.3 When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object.

19.1.4 Where the processing of the personal data is otherwise unlawful.

19.2 When it is necessary to erase the personal data to comply with a legal obligation, and the academy is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

19.2.1 To exercise the right of freedom of expression or information.
19.2.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law.
19.2.3 For public health purposes in the public interest.
19.2.4 For archiving purposes in the public interest, research, or statistical purposes; or
19.2.5 In relation to a legal claim.

19.3 If the academy has shared the relevant personal data with any other organisation, then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

19.4 The DPO must be consulted in relation to requests under this right.

20 Right to Data Portability

20.1 In limited circumstances a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to another organisation.

20.2 If such a request is made, then the DPO must be consulted.

21 Data security

21.1 We will take appropriate security measures against unlawful or un-authorised processing of personal data, and against the accidental loss of, or damage to, personal data.

21.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

21.3 Security procedures include:

21.3.1 Any stranger seen in controlled areas should be reported to a member of SLT.

21.3.2 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always confidential.)

21.3.3 Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

21.3.4 Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

21.3.5 Working away from the school premises – paper documents. Hard copy documents should only be removed from the school site when necessary.

- When this is the case, all reasonable steps should be taken to ensure the safe storage of the documents. Consequently, they should be locked away when unattended e.g. the boot or glove box of a car or lockable briefcase.

21.3.6 Working away from the school premises – electronic working. Transporting, accessing, and storing electronic data away from the school should only be done when necessary. If it is necessary, all reasonable steps should be taken to ensure the safe storage of electronic data. For example, USB and personal device use is prohibited unless they are encrypted, staff should ensure that the personal device, network and or storage area that they are using is secure (use of internet cafes and public computer are not allowed)

21.3.7 Document printing. Documents containing personal data must be collected immediately from printers and not left on photocopiers. Moreover, any documentation that contains personal data must not be left unattended.

21.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

22 Data Protection Impact Assessments

22.1 The academy takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

22.2 In certain circumstances the law requires us to conduct detailed assessments of proposed processing. This includes where we intend to use innovative technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

22.3 The academy will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered. Please see Appendix 1.

22.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

23 Disclosure and sharing of personal information

23.1 We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, and Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

23.2 The Academy will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

23.3 In some circumstances we will not share safeguarding information, such as where it could do further harm to the data subject. Please refer to our Safeguarding and Child Protection Policy.

23.4 Further detail is provided in our Schedule of Processing Activities.

24 Data Processors

24.1 We contract with various organisations who provide services to the Academy.

24.2 In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

24.3 Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the academy. The academy will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

24.4 Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects.

25 Training

25.1 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.

26 Monitoring arrangements

26.1 The DPO is responsible for monitoring and reviewing this policy.

26.2 This policy will be reviewed and updated, as necessary when legislation or guidance alters, Otherwise, this policy will be reviewed every 2 years.

27 Images and Videos

27.1 Parents and others attending Academy events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The academy does not prohibit this as a matter of policy.

27.2 The academy does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, generally, outside of the ability of the academy to prevent.

27.3 The academy asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

27.4 As an academy we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

27.5 Whenever a pupil begins their attendance at the academy, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have either a lawful purpose or consent to do so.

28 CCTV

28.1 The academy operates a CCTV system. Please refer to the academy CCTV Policy.

29 Changes to this policy

29.1 We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

30 Complaints

30.1 Complaints will be dealt with in accordance with the school's complaints policy. In the unlikely event that the complainant remains unsatisfied, complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

31 Contacts

31.1 If you have any enquiries or concerns or would like more information about anything mentioned in this policy, please contact our administration office by telephone on 01380 813796, or email admin@holytrinity.wilts.sch.uk . Alternatively, our data protection officer: Jeremy Shatford by Email: dpo@jeremyshatford.co.uk .

31.2 Further advice and information are available from the Information Commissioner's Office, https://ico.org.uk/or telephone 0303 123 1113

32 Links with other policies

1.1 This data protection policy is linked to our:

- Freedom of information publication scheme.
- Privacy Notices.
- Subject Access Requests.
- Breach
- Retention schedule.
- Online Safety Policy.
- Staff Responsible Use Agreement.
- Safeguarding & Child Protection Policy.

33 Document History

Date	Description
November 2021	Updates to meet revised statutory guidance.

34 Annex - Definitions

Term	Definition
Data	Is information, which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	For this policy includes all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	Means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controllers	Are the people or organisations which determine the purposes for which, and the way, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	Are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	Include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Is any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes, any individual employed by [School/Trust/Academy] such as staff and those who volunteer in any capacity including Governors [and/or Trustees / Members/ parent helpers]

35 Appendix 1 - DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA