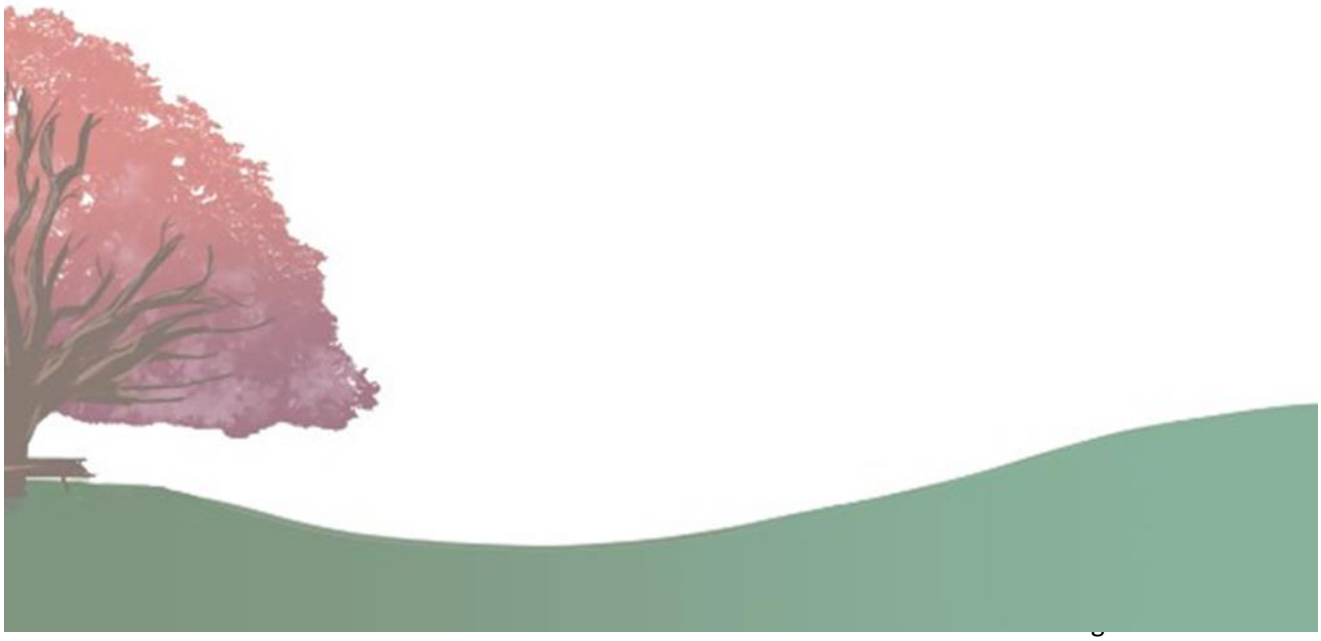
Christ Church CE VC Primary School

"Together we learn - Together we grow - Together we flourish"

Some seeds fell on good earth and produced a harvest beyond wildest dreams.
Matthew 13:8

Data Protection Policy

Date ratified: 18 October 2022
Ratified by: Governing Body
Review date: 18 October 2023



Contents

1 Introduction

1.1 Christ Church CE VC Primary School collects and uses personal information about staff, pupils, parents, and other individuals who have contact with the school. This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory responsibilities.

1.2 We are the Data Controller and as a Public Authority we are required to be registered, along with the name of our data protection officer (DPO), with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

1.3 Our data protection officer is Jeremy Shatford who may be contacted in writing to the school clearly labelled "Data Protection", or by email to dpo@jeremyshatford.co.uk.

2 Purpose

2.1 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018 (DPA) and incorporates the UK General Data Protection Regulation (UK-GDPR), Freedom of Information Act 2000 (FOI) and other related legislation. It will apply to information regardless of the way it is collected, used,

recorded, stored, and destroyed, and irrespective of whether it is held in paper files or electronically.

2.2 All staff involved with the collection, processing and disclosure of personal data will be made aware of their duties and responsibilities and adhering to the guidelines set out in this policy.

3 Governance

3.1 The school controls and processes personal data relating to parents, pupils, staff, governors, visitors, and others, and therefore is a data controller.

3.2 The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

3.3 This policy is the responsibility of the governing body and will be kept under review at least annually but amended earlier when required.

4 Records and Documentation

4.1 The UK-GDPR Article 30 specifies various records of processing activities along with the requirements to have written documentation.

4.2 Christ Church CE VC Primary School will maintain all relevant documentation to be made available to the ICO if required. We will do so through this policy along with:

- Our privacy notices.
- Record of processing activities.
- Our security measures.
- The names and contact details of any person or organization carrying out processing activities on our behalf.
- Retention periods.
- The categories of any recipients that personal data has been disclosed to.

5 What is Personal Data?

5.1 Personal information or data is defined in the UK-GDPR as “any information relating to a natural person who is identified or identifiable, directly or indirectly, with particular reference to an identifier, such as name, ID number, location data, or one or more factors relating to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person”. The person to whom the information relates to is referred to as a “Data Subject”.

6 Data Protection Accountability Obligations

6.1 In addition to the six specific principles shown below an accountability principle runs across all UK-GDPR compliance. This accountability principle places the onus on Christ Church CE VC Primary School as the data controller to comply with the UK-GDPR and to document that fact as well.

6.2 Christ Church CE VC Primary School will, demonstrate our accountability dependent on our circumstances. The following examples show how we demonstrate this:

- The adoption and implementation of certain policies along with maintaining certain documents and contracts.
- Ensure that data protection is embedded within our organisation by design and default.
- Maintain our records of data processing.
- Carry out data protection impact assessments where necessary.
- Record and report personal data breaches.

7 The Six Specific Principles

7.1 Personal data shall be processed fairly and lawfully, and in a transparent manner. ('lawfulness, fairness and transparency')

- We will identify valid grounds under the GDPR (known as a 'lawful Basis') for collecting and using personal data.
- We will ensure that we do not do anything with the data in breach of any other laws.
- We will use personal data in a way that is fair. This means we will not process the data in a way that is unduly detrimental, unexpected, or misleading to the individuals concerned.
- We will be clear, open, and honest with people from the start about how we will use their personal data.

7.2 Personal data shall be collected for specific, explicit, legitimate, and limited purposes ('purpose limitation')

- We will be clear about what our purposes for processing are from the start.
- We will record our purposes as part of our documentation obligations and specify them in our privacy information for individuals.
- We will only use the personal data for a new purpose if either this is compatible with our original purpose, we get consent, or have a clear obligation or function set out in law.

7.3 Personal data shall be adequate, relevant, and limited to what is necessary ('data minimisation')

- We will ensure the personal data we are processing is:

  a) adequate – sufficient to properly fulfil our stated purpose.
  b) relevant – has a rational link to that purpose; and
  c) limited to what is necessary – we do not hold more than we need for that purpose.

7.4 Personal data shall be accurate and where necessary, kept up to date; (accuracy)

- We will take all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact.
- We will keep the personal data updated, depending on what we are using it for.
- Should we discover that personal data is incorrect or misleading, we will take reasonable steps to correct or erase it as soon as possible.
- We will consider any challenges to the accuracy of personal data.

7.5 Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.

- We will not keep personal data for longer than we need it.
- We will agree a retention period to determine how long we keep personal data.
- We will review the data that we hold, and erase or anonymise it when we no longer need it.
- We will consider any challenges to our retention of data recognising individuals' rights to erasure if we no longer need the data.

7.6 Personal data will be processed in accordance with the rights of data subjects under the Data Protection Act 2018.

7.7 Personal data shall be kept secure i.e., protected by an appropriate degree of security ('integrity and confidentiality').

- We will ensure that we have appropriate security measures in place to protect the personal data we hold.

8 Rights of Individuals

8.1 Articles 12 to 23 of the GDPR details the rights of data subjects which seek to protect their fundamental rights and freedoms.

8.2 Our data subjects will be allowed to exercise their rights where they apply which are:

- The right to be informed. The right to know how personal data is used in clear and transparent language by providing privacy notices.
- The right of access. The right of data subjects to know and have access to the personal data held about them (see Subject Access Request).
- The right to data portability. The right to receive and transfer information that the data subject has given, in a common and machine-readable electronic format.
- Though not an absolute right we will consider your right to be forgotten. The right of data subjects to have their personal data erased in certain circumstances.
- The right to rectification. The right to have data corrected where it is inaccurate or incomplete.
- The right to object or to complain about processing where possible.
- The right to restriction of processing. The right to limit the extent of the processing of the data subject's personal data according to their wishes in certain circumstances.
- Rights related to automated decision-making and profiling. You have the right not to be subject to decisions without human involvement.

8.3 There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual orientations
- criminal records

8.4 Christ Church CE VC Primary School and all staff or others who process or use personal information must ensure that they always follow these principles. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school. Any failures to follow the policy can therefore result in disciplinary proceedings.

9 General Statement

9.1 The school is committed to always maintaining the above principles. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected.
- Through our privacy notices Inform individuals when their information is shared, and why and with whom it was shared.

- Check the quality and the accuracy of the information we hold.
- Ensure that information is not retained for longer than is necessary by following our retention policy.
- Have appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure our staff are aware of and understand our policies and procedures.
- Provide and identify, regular training required to enhance staff understanding of the UK-GDPR principles and our practices. This is through staff induction, team meetings, and specific training events including those online.

10 Responsibilities

10.1 The governing body have overall responsibility and accountability for compliance with the DPA and delegates the day-to-day operation to the headteacher.

10.2 The headteacher is responsible for ensuring compliance with the DPA and this policy.

10.3 All members of staff or contractors who hold or collect personal data are also responsible for their own compliance with the DPA and must ensure that personal information is kept and processed in-line with the DPA.

10.4 All staff must check that any personal data that they provide to the school in connection with their employment is accurate and up to date. They must also inform the school of any changes in their personal data that they have provided, e.g., change of address, either at the time of appointment or subsequently.

10.5 Staff should report any unauthorised disclosure, loss of personal data, or other breach of this policy immediately, to minimize potential damage to data subjects, or to the reputation of the school. Failure to report a data breach will be treated as disciplinary matter and may be considered gross misconduct in some cases.

10.6 The school will take appropriate organisation and technical measures to ensure that any third parties who process personal data on behalf of the school, do so in a manner that permits the school to uphold its statutory responsibilities in relation to data protection.

10.7 All staff will receive training on processing personal data, through our induction and as part of our staff development programme.

11 Fair Processing/ Sharing Personal Data

11.1 Christ Church CE VC Primary School has a duty to issue a Privacy Notice to all pupils/parents and staff, this summarises the personal data we hold, why it is held and the other parties to whom it may be passed on to.

11.2 Parents/Carers will always have access to a copy of our Privacy Notice for pupils with a review held at the beginning of each academic year. A copy of this notice will be available on the school website.

11.3 Staff will be issued with a copy of our Privacy Notice for the school workforce on induction and a copy of this notice will also be available in the Staff shared drive.

11.4 If we need to share personal data with third parties, will not do so unless:

- We have received consent to do so, **or**

- We are required to do so by law, **or**
- We have a lawful reason for doing so as outlined in our privacy statement

11.5 It is a criminal offence to obtain knowingly or recklessly, or share (disclose) information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- other members of staff on a need-to-know basis.
- relevant Parents/Guardians.
- other authorities if it is necessary in the public interest, e.g. prevention of crime.
- other bodies, such as the Local Authority and schools to which a pupil may move, where there are legitimate requirements.
- Any other person or organisation where the law, requires us to do so

11.6 The school will not disclose any information from a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else.

11.7 Where there is any doubt, or statutory requirements conflict we will seek additional advice before disclosing personal information.

11.8 When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. So, from time to time we may need to ask parents/carers additional questions, to which only he/she is likely to know the answers. Information will not be provided to other parties, even if related. For example: in the case of divorced parents, it is important that information regarding one party is not given to the other party to which he/she is not entitled.

11.9 Where we are required to share personal data with other agencies, this will be done through secure transfer mechanisms.

11.10 Any person whose details are held by the school is entitled, under the provisions of the DPA, to ask for a copy of all information held about them (or child for which they are responsible). Please see our Subject Access Request Policy/Procedure (SAR) for details on how we deal with Subject Access Requests.

12 Contractors and Tendered services

12.1 The school may point parents to our external contractors where our services are enhanced by doing so. For example: - school.money.co.uk that enables parents to pay online for various services and School Meals providers, for the provision of school meals.

12.2 It is important to understand the relationship between the school and such suppliers please see the following examples:

Example 1

In the case of the school meals provider parents have direct contact to enable them to order and pay for their child's meals. The school meals provider is therefore the data controller for this information and the school is not responsible.

Some children are entitled to free school meals. In this instance the school passes relevant information to the school meals provider, so they know which children to invoice the school for. The school is therefore the controller, and the school meals provider is the processor. The school remains responsible for the data. Save for, where law requires the processor to retain data.

Example 2
The use of schoolmoney.co.uk is a direct agreement between the parent and company so the company is the controller and responsible for all data. The school will where possible provide an alternative for parents who do not wish to enter such agreements. For example, pass a cheque from a parent on to the provider.

13 School Life

13.1 There are many aspects to school life that we must do to teach children to a high standard. We do not need to ask for parental consent for many of these but where we do, we will ask you for it.

14 Information Security

14.1 The school is committed to take the necessary precautions to protect the security of the personal data it is responsible for.

14.2 Access to the school site is restricted and the personal data of pupils that is on display is not visible via the public areas of school reception.

14.3 The school has taken appropriate security measures to protect personal data stored within school buildings from theft, damage, or other unauthorised disclosure.

14.4 The school has taken appropriate measures to protect the security of pupil's and staff information that is stored in onsite information systems, paper records, cloud-based/online systems and in visual/audio media.

14.5 All staff must ensure that:

- personal data is kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- Is saved to the school server, school laptop/desktop or onto One Drive via a School account. Any removable storage is not permitted (this includes USB memory keys, portable hard-drives, SD cards, unencrypted laptops).

14.6 When staff are required to take personal information away from the school site, provisions have been made to support the secure transfer of information and guidance has been issued to staff who may be required to access personal data away from school.

14.7 School IT systems have appropriate security measures in place, with permission and access to personal information controlled, based on the role and responsibilities of staff.

14.8 All mobile devices (including memory sticks, portable hard-drives, and other storage systems) used to manage personal data have been encrypted to an appropriate standard in line with ICO guidance.

14.9 Paper records containing sensitive or confidential data are locked in secure storage spaces, with access controlled by the Headteacher and nominated appropriate staff.

14.10 All staff are committed to ensure that all Personal Data held by school is maintained so that it accurate and of a quality that supports the purpose(s) it has been collected for. Parents/carers are encouraged to support the school in the task of managing personal data for pupils by advising the school office of any changes to personal information in a timely manner.

15 When should personal data be rectified?

15.1 Christ Church CE VC Primary School is committed to ensuring all data we hold is accurate and fit for purpose. We also acknowledge that Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

16 The right to erasure

16.1 The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e., otherwise in breach of the GDPR).
- The personal data must be erased to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

17 Data Protection impact assessments

17.1 The school will adopt a risk-based approach before undertaking higher-risk data processing activities. The school (Data controller) will be required to conduct data protection impact assessments where privacy breach risks are high to analyse, mitigate or minimise the risks to their data subjects.

18 Photographs and Digital Images (including video)

18.1 We use photographs and digital images for a variety of purposes, these include, but are not limited to:

- Capturing development and progress in learning.
- School prospectuses and other publications focussed on promoting the school.
- Assemblies and celebration events.
- Sports day.
- School performances.
- Trips and residential outings.

18.2 Where images of children or staff are used in public areas or made available online via publication on the school website. The school will always seek consent before images are published.

19 Records of achievement

19.1 We encourage children to share their achievements, this may be done where other parents may be present and through wall displays within the classrooms.

19.2 The information shared in this way may include the child's name, age and mark given for a piece of work. In addition, leader boards may be displayed within classrooms that show achievements of individuals in comparison to others.

19.3 These records are generally well known as the information is widely shared within the classroom environment and are assessed as low risk to the data subjects.

20 Publication of School Information

20.1 Certain items of information relating to the school will be made available on the public website, to meet the legitimate needs of researchers, visitors and enquirers seeking to contact the school. Where it is not a legal requirement, personal data will not be published without consent from the individual concerned.

20.2 The GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 cannot give that consent themselves and instead consent is required from

a person holding 'parental responsibility'. UK law will apply, and the school will consider the wishes of the child where it can lawfully do so, and where the child demonstrates competency to express those views.

21 Retention and Disposal

21.1 The school operates a Retention Schedule to determine the length of time that documents containing personal data should be kept for. This schedule is in line with the recommended periods of retention published by the Records Management Society.

21.2 The school will also ensure that when obsolete, information is destroyed in a secure and appropriate manner. Records of destruction will be maintained where the disposal of personal data has been commissioned to third parties.

21.3 All paper documents that contain personal data will be shredded once they are no longer required, accurate and up to date or when the retention period has been met.

21.4 Electronic devices containing personal data will be formatted and destroyed by an approved contractor with a certificate of destruction being presented for each disposal.

22 Personal data breaches

22.1 The ICO defines that a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

22.2 The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.

22.3 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will inform those individuals without undue delay.

22.4 The school will make all reasonable endeavours to ensure that there are no personal data breaches.

- We will ensure you have robust breach detection, investigation, and internal reporting procedures in place.
- We will involve our DPO in the decision-making about the need to notify the ICO or the affected individuals, or both.
- We will keep a record of any personal data breaches, regardless of whether you are required to notify.

23 Complaints

23.1 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).

24 Contacts

24.1 If you have any enquires in relation to this policy, please contact the Deputy Head, Mrs Helen Rutt via the school office who will also act as the contact point for any subject access requests. Alternatively you can contact our DPO by email dpo@jeremyshatford.co.uk.

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

25 Links with other policies

25.1 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.

26 Document History

Date	Description
1/04/2022	Complete revision to update considering legislative changes.