# Castle Hill Primary

# School

# Data Protection Policy

Reviewed: November 2025

Reviewed by: School Business Manager/Data Protection Officer

Approved by: Full Governing Board

Review frequency: Annually

**Contents Page**

## Data Protection Policy - General Data Protection Regulation

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

This document meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018 and the School intends to rely on these as and when appropriate, with particular reliance on paragraph 18, 'Safeguarding of children and individuals at risk' and paragraph 17, 'Counselling'.

### 1. Introduction

In order to work effectively **Castle Hill Primary School** has to collect and use information about people with whom it works. This may include (past, present and future) pupils, parents, teachers, trustees, members of the public, contractors and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government.

All personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by other means. We are all responsible for its safe handling.

This document sets out the principles of data protection, our responsibilities, and the access rights of individuals, as well as information sharing and complaints.

### 2. Scope/ Our Commitment

This policy applies to all staff, governors, contractors, agents, representatives and temporary staff, working for or on behalf of the School. The requirements of this policy are mandatory for all of these parties.

**Castle Hill Primary School** regards the lawful and correct treatment of personal information as critical to its successful operation, maintaining confidence between the school and those it interacts with. The school will ensure that it treats personal information correctly in accordance with the law.

**Castle Hill Primary School** fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act (2018) and the General Data Protection Regulation (UK GDPR).

**Castle Hill Primary School** is committed to ensuring that their staff are aware of data protection policies, legal requirements and that adequate training is provided.

Changes to data protection legislation, under the UK GDPR and DPA, shall be monitored and implemented in order to remain compliant with all requirements.

## 3. Principles of Data Protection

The UK GDPR outlines seven key principles for anyone who processes personal data. These principles form the basis of our approach to processing personal data.

Guide to data protection | ICO

Key definitions of the Data Protection Act | ICO

• ensure that data is fairly and lawfully processed
• process data only for limited purposes
• ensure that all data processed is adequate, relevant and not excessive
• ensure that data processed is accurate
• ensure that data is not kept for longer than is necessary
• process the data in accordance with the data subject's rights
• ensure that data is secure
• ensure that data is not transferred to other countries without adequate protection.

## 4. Responsibilities

**Castle Hill Primary School** is registered as a data controller with the ICO and will renew this registration as required.

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Register of data controllers | ICO

Data breaches shall be notified within 72 hours to the individual(s) concerned and the ICO.

The members of staff responsible for data protection within the School are mainly School Business Manager, Headteacher and SLT. However, all staff must treat all pupil (or other relevant) information in a confidential manner and follow the guidelines set out in this document.

We have appointed Gloucestershire County Council as our Data Protection Officer. They can be contacted on 01452 583619 or schoolsdpo@gloucestershire.gov.uk

## 5. Definitions of Data

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual but need not be sensitive information. The UK GDPR makes

a distinction between personal data and “special category” (sensitive) data. Special category personal data requires stricter conditions for processing.

**Personal data** is Defined in s(1) of the UK GDPR, as ‘data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller’ (the School is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.

**Special Category Data** is information about racial or ethnic origin, sexual life or sexual orientation, biometric and genetic data, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.

## 6. Processing Personal Data

### 6.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school, as a public authority, can perform a **public task,** and carry out its official functions
- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone’s life
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual’s rights and freedoms are not overridden)
- Where the above does not apply we shall request clear **consent** from the individual (or their parent/carer when appropriate in the case of a pupil)

For further detail of which lawful basis is used for each category of data, see the relevant privacy notice.
For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. This is laid out in more detail in point 6.3.

If we offer online services to pupils, such as classroom apps, we intend to rely on Public Task as a basis for processing, where this is not appropriate, we will get parental consent for processing (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

In addition, the UK's Data Use and Access Act 2025 (DUAA), has introduced a category of "Recognized Legitimate Interests" (RLI). This new basis for lawful processing simplifies

the process for certain types of data processing deemed to be in the public interest by removing the need for a balancing test between the data subject's rights and the school's interests.

**6.2 Limitation, Minimisation and Accuracy**
We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

**6.3 Our processing of special categories of personal data and criminal offence data**
As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the General Data Protection Regulation (UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

## 7. Sharing Data

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information on to external authorities, for example local authorities, Ofsted, or the department of health.

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Any proposed change to the processing of an individual's data shall first be notified to them.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**

If a pupil transfers from **Castle Hill Primary School** to another school, their records and other data that relates to their health and welfare will be forwarded on to the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**

If a situation arises where a criminal investigation is being carried out, we may have to forward information on to the police to aid their investigation. We will pass information on to courts as and when it is ordered.

- **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of suspected child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Education division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child's or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

## 8. 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, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, prospectuses newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns or third-party benefactors (such as charities or companies who provide financial support to the school).
- Online on our school website or social media pages/ feeds.

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.

## 9. Data Protection Rights of the Individual

### Data Access Requests (Subject Access Requests)

All individuals, whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

**Castle Hill Primary School**

No charge will be applied to process the request.

### Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

### Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- Where personal data is no longer required for its original purpose, an individual can demand that the processing is stopped, and all their personal data is erased by the school including any data held by contracted processors.

Please note that under the Data Protection Act 2018, schools are entitled to extend this deadline by an additional 2 months, should the Data Protection Officer deem the request challenging and/or complex, this will be explained to the requester within 20 days of the request being submitted.

The DUAA (Data Use and Access Act 2025) also allows schools a “stop the clock” rule, allowing the school to pause the response time if they need more information from the requester. Once the school obtain the information they need, the response time continues.

## 10. Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual’s privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

Risk and impact assessments | ICO

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of their competence in the security of shared data.

## 11. Location of Information and Data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard or office. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical officer.

Sensitive or personal information and data should not be removed from the school site; however, the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced, they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers
- Laptops and USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

## 12. Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance:

IT asset disposal for organisations | ICO

The school uses **<Insert Company Name>** to dispose of sensitive data that is no longer required and there is a cross shredder for the purposes of shredding confidential information on-site.

## 13. Complaints

Complaints about how the school processes data under the GDPR and responses to subject access requests are dealt with using the School's complaints procedure.

## 14. Breach of Policy

Any breach of this policy should be investigated in accordance with our Data Breach process. The School will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.

## 15. Related Policies / Documentation

- Privacy Notice
- Complaints procedure
- Consent form
- CCTV
- Freedom of Information Policy