

# Data Protection Policy



## Chaloner Primary School

Date Policy Approved	March 2019
Review frequency	Every year
Next review date	On or before March 2020
Approving body	Full Governing Body

## **Purpose**

This policy ensures that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provision of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

In line with our statutory duty, we are registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. On induction, we issue Fair Processing Notice to all pupils, parents and staff and governors, which are also on our website to download.

## **What is personal Information?**

Chaloner Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be legal requirements to collect and use information to ensure that the school complies with its statutory obligations.

Personal information is anything relating to a person that identifies them. This includes both physical records and digital records.

At Chaloner Primary School, examples of personal information include:

- Names of staff and pupils.
- Dates of birth.
- Photographs of staff and pupils that are clearly linked to their identity or other personal information about them.
- Addresses.
- National insurance numbers.
- Financial information, such as bank details and tax status.
- Recruitment data.
- Attendance and behavioural information.
- Safeguarding information, including SEN assessments and data.
- School work and marks.
- Medical information, such as medical conditions and GP names.
- Exam results.
- Staff development reviews.
- The purpose for which it holds personal data.
- What data it holds.
- The source of said data.

## **Fair Processing and Privacy Notices**

When we collect information about a child, parent or staff member, we are clear and transparent about how we intend to use it. For example, to facilitate education or to arrange school trips.

In order to do this and comply with the Data Protection Act Principles and we have Privacy Notices in place. The aim of a Privacy Notice is to summarise what information we need and why we are collecting it. We always seek consent in order for us to hold information given.

Privacy Notices are included in all enrolment documentation and on the bottom of any forms used to collect personal information.

## **The Key Data Protection Principles**

In order to protect personal information we- as data controllers and complying with data protection law (as amended by GDPR)- follow several key principles:

- Fair, lawful, and transparent processing.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Data retention periods.
- Data security.
- Accountability.

The information in this policy shows how we comply with all of these principles.

## **Information Security Measures**

Once we acquire personal information about students, parents and staff, both manual and digital records are kept secure. The level of security reflects the potential harm that could result from the loss or misuse of the data. Any security breaches must be reported and will be dealt with by our DPO (Data Protection Officer) Christine Saunders.

Security measures for data protection include:

- Shredding all confidential waste or using confidential waste collection services.
- Strong passwords are used.
- A firewall and virus checker on all computers.
- Computer use monitored through our IT SLA.
- Any personal information held electronically is stored securely, memory sticks are encrypted.
- Disabling any 'auto-complete' settings.
- Telephone calls are held in private areas.
- Access is limited to those individuals who absolutely need to access the data.
- Governor spot check of the security of our storage systems.
- Devices under lock and key when not in use.
- Paper with personal information is not left lying around.

Memory sticks should be avoided to store personal information; where the use is necessary, they must be password protected and fully encrypted. Our IT providers Laurence Jackson School, ensure that hard drives are erased securely if they are physically disposing of them.

### **Special Categories of Personal Data**

This is personal data which is more sensitive and so needs more protection, including information about the individuals:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Genetics
- Health- physical or mental
- Sex life or orientation
- Criminal offences

At Chaloner we take extra precautionary measures to store this information including the use of SIMs and CPOMs.

### **Pupil Subject Access Request**

A pupil, or someone acting on their behalf, has the right to make a request to see any personal data we hold about them and why.

Parents/carers are only entitled to access the personal information held about their child if the child is unable to act on their own behalf, or if the child has given their consent. Even if the child is young, the personal data being held is still their personal data. It doesn't belong to anyone else, including their parents or carer/guardian.

Parents, however, do have the right to see their child's educational records. If you wish to make a subject access request, this needs to be in writing to Mrs Parker.

### **Sharing Personal Information**

There are occasions where sharing personal data with local authorities, other schools, different departments or social services cannot be avoided. It may be that without sharing the data, actions cannot be completed.

For example, we may need to pass on details about a child showing signs of harm to social services, or another school may need to know which pupils will be present at their sports day event.

We will always consider all the legal implications and ensure that we have the ability to share the specified data. We will consider, what is the intention behind sharing? Who requires the data, which data is needed? and what will it be used for?

Consent to share information is part of the Privacy Notice issued when the data was first collected. Letters sent from school that requires providing personal information will have a data protection statement at the bottom where relevant.

## **Holding Data and Keeping it Up to Date**

During the time we hold data about a person, and for as long as it is being used, it is essential that we ensure it remains relevant and accurate. To do this we carry out an audit at least annually

This audit includes:

- A letter at the start of each school year asking parents and pupils to check that their details are correct. This also helps prevent emergency risks, e.g. if an old address or phone number is on record.
- A letter at the start of each school year asking staff and visitors to check that their details are correct.
- As parent phone numbers are regularly changing, in addition to all trip consent forms from parents/carers, we ask for a current phone number so we can amend our record accordingly.
- Any time we become aware that information needs amending, we do so immediately
- Any personal data that is out of date or no longer needed is 'destroyed'. This may involve shredding documents or deleting computer files securely so that they cannot be retrieved.
- Schools follows the disposal of records schedule. This schedule states how long certain types of personal data can be held for until it must be destroyed. Some stipulations are legal obligations while others are best practice.

We are aware that we are violating the Data Protection Act if we keep any data for longer than it is needed.

Chaloner Primary School will only acquire and process data in a manner related to the intended purpose. All forms are scrutinised to determine what may be excessive and decide what information is absolutely critical for the intended purpose.

The publishing of data on our website is in line with statutory requirements.

## **Photographs and Videos**

As part of our school activities, we may take photographs and record images of individuals within our school. Photographs are taken for a variety of reasons but only in accordance with our data protection responsibilities. Staff follow our Acceptable Use Policy at all times when relating to photographic data.

We obtain written consent from parents/carers for photographs and videos to be taken of their child and how we use it. This consent is obtained on entry to the school and reviewed annually. Consent can be refused or withdrawn at anytime. 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. Information about how images are taken, used and stored can also be found on our school website and in our Online Safety Policy and Computing Policy.

## **Our Data Protection Responsibilities**

At Chaloner Primary School, we put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a DPO (Christine Saunders), and ensuring she has the necessary resources to fulfil her duties and maintain her 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.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regular training for staff on data protection law, this policy and any other data protection matters.
- Regular reviews and audits to test our privacy measure and make sure we are compliant.
- Ensure all induction and enrolment for pupils and staff include the Privacy notices and data protection awareness, including the name of our DPO.

## **Personal Data Breaches**

Chaloner Primary School will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, this must be reported to the data protection officer (DPO) Christine Saunders or to the Headteacher Mrs Parker. 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.
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted data about staff or pupils.

## **Complaints**

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the DPO and /or the Information Commissioner (the statutory regulator)

Further advice and information is available from the Information Commissioners' Office [www.ico.gov.uk](http://www.ico.gov.uk) or telephone: 0303 123 1113