



## **Dallimore Primary & Nursery School**

## **GDPR and Data Protection Policy**

# **Contents**

Page 3 – Policy & Procedures

Page 9 – Glossary

Page 11 – Withdraw Consent letter

## Overview

Dallimore Primary and Nursery School is committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data and we take that very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

The school will be responsible for the day to day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

## What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the Eu on 31 December 2020.

The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

## Who does it apply to?

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and proposed provisions in the Data Protection Act 2018.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

## What is Data?

Any information that relates to a living person that identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEND or health needs. Information about other family members may also be on the school file.

Privacy Notices that explain how data about specific groups or activities is used and stored are also available. These can be obtained from school and links on the website to UK GDPR compliance.

## **What are the key principles of the UK GDPR? Lawfulness, transparency and fairness**

Schools must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent we have a form to complete to allow us to process your request. There are some times when you cannot withdraw consent as explained in 'Data Subjects' Rights'.

### **Collect data for a specific purpose and use it for that purpose**

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

### **Limited collection**

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

### **Accuracy**

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the individual school.

### **Retention**

A retention policy is in place that governs how long records are held for.

### **Security**

We have processes in place to keep data safe. That might be paper files, electronic records or other information. These include our Retention of Records Schedules, IT Acceptable Use Policy and GDPR code of conduct principles for instance.

### **Who is a 'data subject'?**

An individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

## Data subjects' rights

Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

## Subject Access Requests

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if the request is complicated or the data cannot be accessed.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information by paper or electronic form.

If you wish to complain about the process, please see our Complaints Policy and later information in this DPA policy.

## Who is a 'Data Controller'?

The school is the Data Controller. They have ultimate responsibility for how the data is managed. They delegate this processing to individuals to act on their behalf.

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

## Who is a 'Data Processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party

company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the Local Authority.

Data Controllers must make sure that Data Processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

## Processing data

The schools must have a reason to process the data about an individual. Our Privacy Notices set out how we use data. The UK GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

## Data Sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared. The basis for sharing or not sharing data is recorded in school.

## Breaches & Non Compliance

If there is non compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed.

Protecting data and maintaining Data Subjects' rights is the purpose of this policy and associated procedures.

## Consent

As a trust, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the UK GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

## Consent and Renewal

On the school websites we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent, where required, and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

## For Pupils and Parents/Carers

On joining the school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection/consent form.

The contact and consent form is reviewed on an annual basis. It is important to inform school if details or your decision about consent changes. This is the obligation of the parent or carer to notify the school of changes.

## Pupil Consent Procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child as required.

## Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. A sample form to withdraw consent that parents and carers can use is at the end of this document. However where more than one person has the ability to provide or withdraw consent the school we will consider each situation on the merits and within the principles of UK GDPR, along with child welfare, protection and safeguarding principles.

## CCTV Policy

Please also see the CCTV Policy. We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:

- Detection and prevention of crime
- School staff disciplinary procedures
- Pupil behaviour and exclusion management processes

## Data Protection Officer

We have a Data Protection Officer whose role is:-

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- to monitor compliance with the UK GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- To be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the UK GDPR

Our DPO is **John Walker** whose contact details are below:

Address: 6 Delamore Park, Cornwood, Ivybridge, PL21 9QP

Email: [info@phplaw.co.uk](mailto:info@phplaw.co.uk)

## Physical Security

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

All Staff who are responsible for locking away personal and sensitive data must take due care to prevent data breaches and safeguarding of this data.

## Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

## Complaints & the Information Commissioner Office (ICO)

There is a right to complain if you feel that data has been shared without consent or lawful authority. You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details

about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: [casework@ico.org.uk](mailto:casework@ico.org.uk) Helpline: 0303 123 1113 web: [www.ico.org.uk](http://www.ico.org.uk)

## Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the Data Protection Officer every 12 - 24 months and the School will review this policy on a 2 – year cycle.

**Policy Date: October 2023**

**Review Date: Autumn 2025**

## Glossary

**Automated Decision-Making (ADM):** when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

**Automated Processing:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

**Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

**Data Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

**Data Subject:** a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

**Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

**Data Protection Officer (DPO):** the person required to be appointed in public authorities under the GDPR.

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

**Explicit Consent:** consent which requires a very clear and specific statement (not just action).

**General Data Protection Regulation (GDPR):** General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

**Personal data** is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, 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. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**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 transmitted, stored or otherwise processed.

**Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

**Privacy Notices:** separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

**Processing** means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

**Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

**Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

**Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

# Appendix

## Withdrawal of consent on behalf of a pupil

I, .....(parent/ carer name), withdraw consent in respect of ..... (pupil Name) for Dallimore Primary & Nursery School to process their personal data. I withdraw consent for the following process:

.....  
.....  
.....

which was previously granted.

I confirm that I am ..... (Parent/Carer) and that I have parental responsibility for the pupil.

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

### Received by school

School staff name:

Dated:

Actions: