

GDPR Policy

KINGSKERSWELL C OF E PRIMARY SCHOOL



Achieve, Believe and Create Together

Jeremiah 29:11

For I know the plans I have for you, plans to prosper you and not to harm you, plans to give you **HOPE** and a **FUTURE**.

Approved by: Amy Vine
& Adam Devine

Date: 4th July 2025

Policy Date on: Date 16th June 2021

Next review due by: Date 4th July 2026

1. Introduction

This Data Protection Policy sets out how the School handles the personal data processed by the School. We process personal data about school staff, pupils, parents, governors and Trustees. Further information about the personal data we process can be found in our Privacy Notices which are available in reception and on our school website.

This Policy applies to all School employees, Governors and Trustees. You must read, understand and comply with this Policy when processing personal data on behalf of the School.

Please contact the School Data Protection Officer with any questions about the operation of this policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed.

2. What is Personal Information?

Personal information is defined as data which relates to a living individual who can be identified from that data, or other information held. Personal information can therefore include staff and pupil records, names and addresses, examination marks, references, sensitive data, personnel and much more.

3. Data Protection Principles

Anyone processing personal data must comply with the principles of data processing as set out in the GDPR. These provide that personal data must be:

- a) processed lawfully, fairly and in a transparent manner;
- b) collected only for specified, explicit and legitimate purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- d) accurate and where necessary kept up to date;
- e) not to be kept in a form which permits identification for longer than is necessary for the purpose for which the data is processed;
- f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- g) not be transferred to other people or organisations situated in countries without appropriate safeguards taking place;
- h) made available to data subjects and so as to allow data subjects to exercise their rights and requests.

4. Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

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 or another person i.e. to protect someone's life

The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**

The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden

The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

The data has already been made **manifestly public** by the individual

The data needs to be processed for the establishment, exercise or defence of **legal claims**

The data needs to be processed for reasons of **substantial public interest** as defined in legislation

The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**

The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

The data has already been made **manifestly public** by the individual

The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**

The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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.

5. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

We need to liaise with other agencies – we will seek consent as necessary before doing this

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

6. Transparency

The GDPR requires the school to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. This information is available in our Privacy Notices. Our Privacy Notices set out how we will use, process, disclose, protect and retain personal data.

7. Data Subjects Rights and Requests

Data subjects have rights when it comes to how we handle their personal data. These include rights to:

withdraw consent to processing at any time;

receive certain information about the Trust's processing activities;

request access to their personal data that we hold;

prevent our use of their personal data for direct marketing purposes;

ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

restrict processing in specific circumstances;

challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

request a copy of an agreement under which personal data is transferred outside of the EEA;

object to decisions based solely on automated processing, including profiling;

prevent processing that is likely to cause damage or distress to the data subject or anyone else;

be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

make a complaint to the supervisory authority;

in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format;

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

You must immediately forward any request for personal data you receive to the school or DPO.

8. Reporting a Personal Data Breach

The GDPR requires us to notify any personal data breach to the applicable regulator and, in certain instances, the data subject.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact DPO. You should preserve all evidence relating to the potential Personal Data Breach.

9. Data Security

The School has put in place appropriate procedures and measures to protect the personal data we process. These include:

- a) All visitors to the School must be signed in and will be issued with a visitor's pass. If you notice a stranger on premises without a visitor's badge, please report your concern to the school;
- b) Confidential Waste is shredded by the school or an approved confidential waste company;
- c) Home Working, when handling confidential data is secure at all times and meets guidelines. Sensitive data is prohibited from being taken from site unless for the purpose of a meeting off site
- d) Laptops and computers are encrypted to increase security;
- e) No financial data (card details) stored when payments made by parents/staff via School Money system;

10. Photographs and Videos

The School will gain consent from the parent/carer when the child starts school for photographs and videos by the School. Our consent form will set out the different uses we may have for the photographs and videos and individuals can opt to consent for each, some of, or none of the proposed uses. There will be further consents upon individual events/trips.

Parents, carers and others attending events are permitted to take photographs and videos for domestic purposes. However, the School does not agree to photographs or videos being used for other purposes. Parents, carers and others are requested not to post images or videos which include other children on any form of social media such as Facebook, Twitter and Instagram.

11. Legislation and guidance

This policy meets the requirements of the:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)

[Data Protection Act 2018 \(DPA 2018\)](#)

It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](#).

It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

12. Staff responsibility

Staff are responsible for:

Collecting, storing and processing any personal data in accordance with this policy

Informing the school of any changes to their personal data, such as a change of address

Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

13. Data Protection Officer

The school Data Protection Officer (DPO) can be contacted at admin@kingskerswell.devon.sch.uk or 01803 873398.

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Appendix 1

GDPR Policy Declaration

To be complete by all employees, agency staff, contractors and other relevant staff who process personal data on behalf of Devon County Council.

Managers must keep a copy of the signed Declaration on the employees central personnel or other relevant and accessible file for non employees.

Declaration

I confirm that I have read, understood and will adhere to Devon County Council's GDPR Policy.

Signed _____

Printed _____

Line Manager's Name _____

Phase _____

Service _____

Date _____