# Data Protection Policy

**Head Teacher: Joanne Bruce-Carter**

**Chair of Governors: David Lovelock**

Tadley Primary School
learning for life

**Date: Spring 2026**

**Review Date: Spring 2027**

## Our Vision

At Tadley Community Primary School, we are passionate about equipping our children with the personal characteristics and educational outcomes for their successful futures. Our vision for each child is to develop an active curiosity of their world, discover their own interests and talents, and grow in their own confidence and love of learning. We do this by providing children with an irresistible invitation to learn through our knowledge-rich and diverse curriculum.

**Learning for Life the Tadley Way!**

**Pride, Community, Diversity and Kindness**

## Aims

Tadley Community Primary School collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer, who may be contacted at adminoffice@tadley.hants.sch.uk

The school issues Privacy Notices (also known as Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

## Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

## What is Personal Information/ Data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

## Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive

4. Personal data shall be accurate and where necessary, kept up to date

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.

## Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

## Commitment

Tadley Primary School is committed to maintaining the principles and duties in the GDPR at all times. Therefore, the school will:

- Inform individuals of the identity and contact details of the data controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this
- If the school plans to transfer personal data outside the EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Ensure that personal information is not retained longer than it is needed

- Ensure that when information is destroyed that it is done so appropriately and securely
- Share personal information with others only when it is legally appropriate to do so
- Comply with the duty to respond to requests for access to personal information
  (Known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures

## Breaches

If personal data we handle is lost, destroyed, altered, disclosed, accessed or put beyond use when it shouldn't be, this is a Personal Data Breach.

A personal data breach can occur accidentally or intentionally, and can be caused by staff, by an external threat (including cyber incidents), or anyone else.

- Report the breach or incident internally;
- Record the breach or incident;
- Assess the risk;
- Contain and recover;
- Notify the ICO of the breach (if applicable);
- Notify the affected Data Subjects of the breach (if applicable);
- Review;
- Implement any necessary changes to prevent reoccurrence.

As soon as you become aware of a breach, or possible breach, report it to the Data manager/DHT or SBM/HT in their absence, who will lead on the breach response, including informing the Data Protection Officer of the breach and keeping them updated on the investigation and actions. The report will be made as soon as possible even if the breach is discovered outside of normal working hours.

Consider what harm could come from the breach, including who could be harmed, how they could be harmed, and how severe the harm could be, as well as how likely it is the harm will happen. This risk assessment, based on severity and likelihood, will depend on the types of information involved (how sensitive is it, what could be done with it?), how much information is involved, and how exposed the data is, as well as the individual circumstances of the data subjects (that the data is about).

Examples:

If a laptop has been lost, if it is encrypted there is a very small chance of any data being accessed. But if hard copy documents have been lost or left unattended, they are much more likely to be accessed and read.

If personal data is included in an email by accident, the data may be at more risk of being misused if the email has gone to a member of the public, rather than to another school.

Accidentally disclosing an address might not pose a risk to most data subjects, but it could be very high risk for someone who is escaping domestic violence, or for the adoptive family of a child.

Take reasonable actions to contain the risks, and/or recover the data, if possible. Containment and recovery actions could include, as appropriate:

• Attempting to find lost devices or paperwork;

• If devices have been stolen, report this to appropriate law enforcement agencies e.g. police.

• If a breach or incident is still occurring, for example, due to an ongoing IT issue, then IT will take appropriate steps to minimise the breach, such as closing down an IT system or server. In the event of a Cyber-attack, immediately report to the Action Fraud line on 0300 1232040.

• Warning staff and third parties such as the County Council, to be aware of any "phishing" attempts that might be linked to personal data that has been accessed by criminals/unauthorised people;

• If data has been sent to, or shared with, someone it shouldn't have been, consider if you can contact them to recover the data. Bear in mind that "recall" doesn't usually work on externally sent emails;

• If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use;

• If the data breach or incident includes any entry codes or IT system passwords, change these immediately and inform the relevant agencies and members of staff;

• Contacting the Local Authority Communications Division if part of the crisis service, so that they can be prepared to handle any press enquiries.

**Data Breach Log**

| Action | Give dates, initials and links to docs where appropriate |
|---|---|
| Date and time of discovery | |
| Date and time of occurrence | |
| What happened | |
| Immediate steps taken to contain the breach, e.g., changing passwords, shutting computers down, halting network traffic, restore data from backups | |
| Acknowledge breach by thanking informant for information – log it here | |
| Inform DPO 01189813805 | |
| Assess Risk: | [Consider how many people are affected, what type of data is involved, how could people be harmed, and how likely are they to be harmed?] |
| Necessary to inform ICO? 0303 1231113 | |
| Date and time reported to ICO | |
| Necessary to inform data subjects? | |
| Data subjects informed? | |
| Law enforcement agencies e.g. police informed? | |
| Any other third parties informed? | [Consider banks, suppliers, anyone else who needs to know about the breach.] |
| Review: | [Consider what was in place that should have prevented the breach, and why it failed, how could further breaches be prevented, how have we helped the people affected? Should we improve security, procedures, training, etc.?] |
| Steps taken to avoid reoccurrence | |
| Concluding letter | |
| SLT / Governors de brief | |
| Report completed by | |

## Training

Staff will receive annual training on data protection practices to ensure we are compliant with GDPR and data protection rules.

SAR & FOI

Timescales: SARs will be responded to as soon as possible, and **within one month at the latest**. In the case of complex or multiple requests an extension of up to an extra two months can be applied, but the requestor will be informed of the extension within the first month. The calculation of time will commence once the SAR is determined as valid. An acknowledgement will be sent to the requestor as soon as possible to inform them that the SAR has been received, the start date, and that it is being processed.

Under the Freedom of Information Act (FOIA), public authorities are required to respond to FOI requests within 20

working days from the date the request is received.

**Request form**

Section 1- Requestor details

Title (Mr /Mrs /Miss /Ms /Dr /Rev etc):

Surname/Family Name:

First Name(s) Maiden/Former Name(s) (if applicable):

Date of Birth (dd/mm/yyyy):

Home Address (Include Postcode):

Name of person making request on behalf of data subject (if applicable):

Surname/Family Name:

First Name(s) Relationship to data subject:

Preferred alternative address for correspondence (if applicable):

Contact telephone number Contact e mail address:

Section 2- About your request

What records that you believe we hold would you like access to:

Have you made a request for this information before? (Yes/No) If Yes, could you please provide date of request? (dd/mm/yyyy)

Where do you want to view your information? For example in person, or be sent a paper copy to your home or alternative address or be sent a copy in a specific electronic format to an e mail address (if this is your preferred option we would encrypt the file to keep it secure) :

Do you need any other help with this request? (Please specify below).

Section 3 - Proof of identity

Establishing Proof of Identity

If we have a verified current address for you on our systems we will contact you at that address and ask you to confirm that the request has come from yourself. If this is not possible, we will ask for documentary evidence to verify you are who you say you are.

Section 4 – Declaration (To be signed by the Requestor)

The information, which I have supplied in this application, is correct, and I am the person to whom it relates/I have the right to make this request on their behalf (delete as appropriate).

Signature

Date

Information published on our website is free, although you may incur costs from your Internet service provider. If you don't have Internet access, you can access our website using a local library or an Internet café.

If however your request means that we have to do a lot of photocopying or printing, the following charges will apply:
• 5p per single side of A4,

• 10p per single side of A3.

• plus any postal charge at the current rate applied by Royal Mail.

For a priced item such as some printed publications we will let you know the cost before fulfilling your request. Where there is a charge this will be indicated on application on an individual basis.

## Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

## Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every year. The policy review will be undertaken by the Data Protection Officer, Headteacher, and Governing Body.

## Contacts

If you have any enquires in relation to this policy, please contact the School Office who will also act as the contact point for any queries or concerns.

Relevant legislation includes, but is not limited to:

• UK General Data Protection Regulation (UK GDPR);

• Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for;

• Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing ("marketing" includes fundraising and promoting an organisation's aims, not just selling.)

• Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.

• Environmental Information Regulations 2004

• Human Rights Act 1998

• Computer Misuse Act 1990, which covers unauthorised access to, and use of, computers and computer materials. • Education (Pupil Information) Regulations 2005 which gives parents the right to access their child's education record.

• The School Attendance (Pupil Registration) (England) Regulations 2024 Page 5 of 33 Copyright: Education Data Hub CONTROLLED Issued: April 2025 St. Edward’s Royal Free Ecumenical Middle Data Protection Framework: Data Protection Policy School

• Protection of Freedoms Act 2012 – for further details see our Protection of Biometric Information document.

• The Data (Use and Access) Bill (anticipated to be passed in 2025)

• Children's Wellbeing and Schools Bill (anticipated to be passed in 2025)