Tadworth Primary School

Data Protection Policy

Summer 2018

Tadworth Primary School Data Protection Policy

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors, contractors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions 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.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissions Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of 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'

3. Definitions

Term	Definition
Personal Data	Any information relation to an identified, or identifiable, living individual. This may include the individuals: • Name (including initials) • Identification number • Location data • Online identified, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accident or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data in relation to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1. Governing Body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2. Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.3. All staff

Staff are responsible for:

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

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

5.3.3. Contacting DPO@tadworthps.surrey.sch.uk in the following circumstances:

5.3.3.1. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

5.3.3.2. If they have any concerns that this policy is not being followed

5.3.3.3. If they are unsure whether or not they have a lawful basis to use personal data in a particular way

5.3.3.4. 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 European Economic Area

5.3.3.5. If there has been a data breach

5.3.3.6. Whenever they are engaging in a new activity that may affect the privacy rights of individuals

5.3.3.7. If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy set out how the school aims to comply with these principles.

7. Collecting personal data

7.1. Lawfulness, fairness and transparency

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

7.1.1. 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

7.1.2. The data needs to be processed so that the school can comply with a legal obligation

7.1.3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life

7.1.4. The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions

7.1.5. 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)

7.1.6. 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 one of the special category conditions for procession which are set out in the GDPR and the Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parent consent (except for online counselling and preventative services).

7.2. Limited, 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 Information and Records Management Society.

8. Sharing personal data

We will not normally share personal data with anyone else, but we may do so where:

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

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

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

8.3.1. Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

8.3.2. Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

8.3.3. Only share data that the supplier or contractor needs to carry out their services, and information necessary to keep them safe while working with us.

We may also share personal data with emergency services and local authorities to help them respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1. Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

9.1.1. Confirmation that their personal data is being processed

9.1.2. Access to a copy of the data

9.1.3. The purposes of the data procession

9.1.4. The categories of personal data concerned

9.1.5. Who the data has been, or will be, shared with

9.1.6. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

9.1.7. The source of the data, if not the individual

9.1.8. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should be submitted in writing by email to DPO@tadworthps.surrey.sch.uk. They should include:

9.1.9. Name of individual

9.1.10. Correspondence address

9.1.11. Contact number and email address

9.1.12. Details of the information requests

If staff receive a subject access requests they must immediately forward it to dpo@tadworthps.surrey.sch.uk.

9.2. 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 this 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.

9.3. Responding to subject access requests

When responding to requests, we:

9.3.1. May ask the individual to provide two forms of identification

9.3.2. May contact the individual via phone to confirm the request was made

9.3.3. Will respond without delay and within 1 month of receipt of the request

9.3.4. Will provide the information free of charge

9.3.5. May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or voluminous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

9.3.6. Might cause serious harm to the physical or mental health of the pupil or another individual

9.3.7. Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests

9.3.8. Is contained in adoption or parental order records

9.3.9. Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have a right to complaint to the ICO.

9.4. 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 (see section 7), individuals also have the right to:

9.4.1. Withdraw their consent to processing at any time

9.4.2. Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)

9.4.3. Prevent use of their personal data for direct marketing

9.4.4. Challenge processing which has bene justified on the basis of public interest

9.4.5. Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

9.4.6. Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

9.4.7. Prevent processing that is likely to cause damage or distress

9.4.8. Be notified of a data breach in certain circumstances

9.4.9. Make a complaint to the ICO

9.4.10. Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise this rights to DPO@tadworthps.surrey.sch.uk. If staff receive such a request, they must immediately forward it to that email address.

10. Parent requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school dates of receipt of a request

11. 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 for photographs and videos to be taken of their child for communication, marketing and promotional materials.

Uses may include:

11.1. Within school on notice boards and in school magazines, brochures, newsletter, to identify your child's belongings or needs etc.

11.2. Outside of school by external agencies such as the school photographer, newspapers, campaigns.

11.3. Online on our school website.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete all photographs or videos of your child and not distribute them any further.

When using photographs and videos in this way, we may include other personal information, such as their name.

12. Data Protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities including:

12.1. Appointing a suitable person to respond to any complaints or Subject Access Requests

12.1. 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 (see section 6)

12.2. Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies

12.3. Integrating data protection into internal documents including this policy, any related policies and privacy notices

12.4. Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

12.5. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

12.6. Maintaining records of our processing activities, including:

12.6.1. For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

12.6.2. For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

13. Data Security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

13.1. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

13.2. Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

13.3. Passwords that are at least 8 characters long containing letters and numbers are used to access school computers and laptops. Staff and pupils are reminded to change their passwords at regular intervals.

13.4. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

13.5. Staff, pupils and governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use policy – ICT Code of Conduct)

13.6. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred paper-based records, and overwrite, or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we

will follow the procedure set out in appendix 1. 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:

15.1. A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for pupil premium

15.2. Safeguarding information being made available to an unauthorised person

15.3. The theft of a school laptop containing non-encrypted personal data about pupils

16. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

The Head and Bursar are responsible for monitoring and reviewing this policy.

The policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the Full Governing Body for review.

18. Links with other Policies

This data protection policy is linked to our:

- Freedom of Information Publication Scheme
- Staff Code of Conduct and ICT code of conduct
- E-Safety Policy
- Privacy Notice – Pupils
- Privacy Notice – Workforce
- Use of Photographic and video equipment by parents and carers

Policy reviewed	Summer 2018
Date of Governor approval	11 July 2018
Review date	Summer 2020

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately email DPO@tadworthps.surrey.sch.uk

2. The report will be investigated and a determination will be made on whether a breach has occurred. To decide, it will be considered whether personal data has been accidentally or unlawfully:

   2.1. Lost

   2.2. Stolen

   2.3. Destroyed

   2.4. Altered

   2.5. Disclosed or made available where it should not have been

   2.6. Made available to unauthorised people

3. The Headteacher and Chair of Governors will be made aware of the outcome

4. All reasonable efforts will be taken to contain and minimise the impact of the breach.

5. The potential consequences will be assessed, based on how serious they are and how likely they are to happen

6. A decision will be taken on whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. When deciding, the following will be considered:

   6.1. Whether the breach is likely to negatively affect people's rights and freedoms; and

   6.2. whether the beach is likely to cause them any physical, material or non-material damage (e.g. emotional distress) including through:

      6.2.1. loss of control over their data

      6.2.2. discrimination

      6.2.3. identity theft or fraud

6.2.4. financial loss

6.2.5. unauthorised reversal or pseudonyminsation (for example, key-coding)

6.2.6. damage to reputation

6.2.7. loss of confidentiality

6.2.8. any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the ICO must be notified.

7. The decision (either way) will be documented) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.

8. Where the ICO must be notified, this will be completed via the 'report a breach' page of the ICO website within 72 hours. As required, the following information will be included:

8.1. A description of the nature of the personal data breach, including, where possible:

8.1.1. The categories and approximate numbers of individuals concerned

8.1.2. The categories and approximate number of personal data records concerned

8.2. The name and contact details of the person who has investigated this on behalf of the school

8.3. Any description of the likely consequences of the personal data breach

8.4. A description of the measures that have been, or will be, taken to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

9. If all the above details are not yet known, as much as possible will be reported within 72 hours. The report will explain that there is a delay, the reasons why, and when further information is expected. The remaining information will be submitted as soon as possible.

10. The risk to individuals will be assessed, again based on the severity of the likelihood of potential or actual impact. If the risk is high, all individuals whose

personal data has been breached will be promptly notified. The notification will set out:

10.1. The name and contact details of the person who has investigated this on behalf of the school

10.2. A description of the likely consequences of the personal data breach

10.3. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

11. Any relevant third parties who can help mitigate the loss to individuals will be notified – for example, the police, insurers, banks or credit card companies.

12. Each breach, irrespective of whether it is reported to the ICO will be documented. For each breach, this record will include the:

12.1. Facts and cause

12.2. Effects

12.3. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

A log of all breaches will be maintained.

13. The person who investigated this on behalf of the school and the Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.