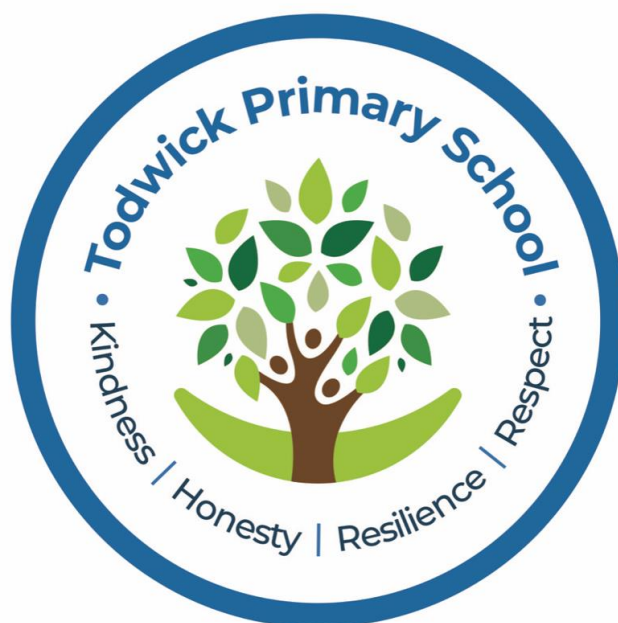


TODWICK PRIMARY SCHOOL DATA PROTECTION POLICY



Policy Date: May 2026

Governor Responsible: Chair of Governors

School Data Protection Officer: Tim Pinto (The E-safety
Office)

General Data Protection Regulation

Our Commitment:

Todwick School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA). <https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/>

Vita interests – the processing is necessary to protect someone's life.

Public Task – the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

Legitimate interests – the processing is necessary for our legitimate interests or the interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

(a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.

(c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

The members of staff responsible for data protection are mainly Alice Deeley and Donna Anderson. Teacher Lucie Singh-Bhatti is the school's DPO. However all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.

The school is also committed to ensuring that all staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:

<https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/>

The requirement is to notify the ICO of any personal data breaches that present a "risk" to the data subject. They should only be reported to the individual and the ICO if they present a "High Risk". Those breaches that do not present a likely risk are not required to be reported but should be logged.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: <https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/>

These are the principles as laid out in the old Data Protection Act 2018. They are now:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be communicated in a form understandable by those defined as 'Children' under the legislation. <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/>

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them. Under no circumstances will the school disclose information or data: recorded by the pupil in an examination" without disclosing it to the exam board, or a marker, moderator, or the police / court where required.

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an a data protection impact assessment as required by law.

Of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be communicated to Alice Deeley, Headteacher, Todwick Primary School

• Right to be Forgotten:

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This is be stored in the main office with the medical coordinator Tracy Radford.

Sensitive or personal information should only be removed from the school site when staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils. This data should only be electronic on school Laptops which are securely protected

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- USB sticks should not be used to transport data between home and school. Laptops only should be used.

Data Disposal:

The secure disposal of redundant hardware and data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner in accordance with ICO guidance. Such disposal companies are sourced through our current IT provider.