Tickhill Estfeld Primary School

Common Lane, Tickhill, Doncaster DN11 9JA
Telephone: 01302 744275

GDPR Policy 2026/27

1.0 Aims:

The school aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be a member of staff, pupil, parent, school governor, visitor, contractor, consultant, a member of supply staff or other individual of the school is done so in accordance with the General Data Protection Regulations (GDPR) and the provision of the Data Protection Act 2018 as set out in the current Data Protection Bill. This policy will be reviwed in line with the implementation of this new legislation.

This policy applies to all personal data collected, stored, processed and destroyed by the school regardless of whether it is in paper or electronic formal, or the type of filing system it is stored in, and whether the collection or processing data was, or is, in anyway automated

2.0 Legislation and Guidance:

This policy meets the guidance of GDPR and the provisions of the DPA 2018. It is based on guidance covered by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It is also based on the ICO's guidance on GDPR and information provided.

This policy meets the requirments of the Protection of Freedom Act 2012, ICO's code of practice in relation to CCTV, and the DBS code of practice in relation to handling sensitive information. This policy also complies with the Education (Pupil Information) (England) Regulations 2005 which gives parents the right to access their childs education record.

3.0 Definition:

Term	Definition
The school	Refers to Tickhill Estfeld Primary School throughout this policy
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data.

Data processor	A natural or legal person, public authority, agency or other body which process personal data on behalf of the Controller, following the Controllers instruction
Data subject	The identified or identifiable individual whose personal data is held or processed.
Consent	Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by a statement or clear affirmative action, signifies agreement to the processing personal data relating to him or her.
Personal data	Any information related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particularly by reference to an identifier such as a: o name; o an identification number; o location data; o an online identifier or o one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special categories of personal data	Personal data which is more personal and so needs more protection including information about a individuals: o racial or ethnic origin; o political opinion; o religious or philosophical beliefs; o trade union membership; o genetics o biometrics (such as fingertip, retina and iris patterns) where used for identification purposes o health – physical or mental o sex life or sexual orientation o history of offences, convictions or cautions[1]

[1] Note: whilst criminal offences are not classed as "sensitive data" with GDPR within this policy we have included them as such as an acknowledgement of the care needed with this data set.

Processing	Any operations or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storing, adaptation or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing can be automated or manual.
Data breach	A breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4.0 Data Controller:

Tickhill Estfeld Primary processes personal data which relates to parents, pupils, staff, governors, visitors and others, and therefore is a data controller and data processor.

5.0 Roles and Responsibilities:

This policy applies to all staff employed at Tickhill Estfeld Primary School, school governors and to external organisations or individuals working on schools behalf, Staff who do not comply with this policy may face disciplinary action.

5.1 The Full Governing Body

The Full Governing Body has overall responsibility for ensuring Tickhill Estfeld Primary School complies will all relevant data protection obligations.

5.2 Data Protection Officer

The Headteacher will appoint a Data Protection Officer. As per Article 39 of the GDPR, the DPO must:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, pupils etc)
- The DPO must keep a record of those staff who have attended Data Protection training
- The DPO reports to the Headteacher or Business Manager
- The DPO operates independently and will not be dismissed or penalised for implementing the obligations associated with the role of DPO, as set out in the regulations or any guidance
- Adequate resources are provided to enable the DPO to meet their GDPR obligations

The Data Protection officer for Tickhill Estfeld Primary School is:

- Mr Tim Pinto

and is contactable via telephone on 0113 266 0880

The DPO is responsible for overseeing the implantation of this policy.

The DPO will provide an annual report of the school's compliance and risk issues directly to the full governing body and will 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.

5.4 Headteacher:

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

5.5 All staff (regardless of role)

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 eg name, address, telephone number or bank details etc
- Contacting the DPO:
  - 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 following
  - If they are unsure whether or not they have the 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 data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that affect the privacy rights of individuals.
  - If they need help with contracts or sharing personal data with third parties

6.0 The GDPR Data Protection principals

The GDPR is based on 6 data protection principles that school must comply with. These are that data must:

- Process lawfully and in a transparent manner
- Collected for specific, explicit and legitimate purpose
- Adequate, relevant and limited to what is necessary to fulfil the purpose for which it is processed
- Accurate, and where necessary, kept up to date
- Kept for no longer than is necessary for which it is processed
- Processed in a way that ensures it is appropriately secure

7.0 Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- The individual (or their parent/carer when in the appropriate in the case of a pupil) has given clear consent.
- The data needs to 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 eg 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, and carry out its official function
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedom are not overridden).

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

These are where:

- The individual (or their parent/carers when appropriate in the case of the pupil) has given explicit consent.
- It is necessary to fulfil the obligation of controller or of data subject.
- It is necessary to protect the vital interests of the data subject.
- Processing is carried out by foundation or not-for-profit organisation (includes religious, political, philosophical organisations and trade unions).
- The personal data has manifestly been made public by the data subject.
- There is an establishment, exercise or defence of a legal claim.
- There is a reason of public interest in the area of public health.
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.
- There are archiving purposes in the public interest.
- The Government has varied the definition of a special category.

Whenever we first collect personal data directly from individuals, school will provide them with the relevant information required by data protection law, in the form of a privacy notice, which can be found on the school website. Hard copies are available upon request.

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 in our privacy notices.

If we wish 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 personal data is no longer required, staff must ensure it is deleted. This will be done in accordance with the school's document retention policy, which it states how longer particular documents should be kept, and how they should be destroyed.

8.0 Sharing Personal Data

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

- There is an issue with a pupil, parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies or services - we will seek consent as necessary before doing this where possible.
- Our suppliers or contractors needs data to enable us to provide services to our staff and pupils – for example IT companies, payroll services.
  When doing this, we will:
  - Only appoint supplies or contractors which can provide sufficient guarantees that they normally comply with data protection law, and have satisfactory security measures in place.
  - 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 personal data we share.
  - 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 will also share personal data with law enforcement and government bodies where we are legally required to do so for:

- Prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC
- Social Services
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes as long as the personal data is sufficiently anonymised or consent has been provided.

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 in accordance with data protection law, and will consult with affected individuals first.

9.0 Individual Rights under GDPR

9.1 Subject access requests

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

- Confirmation that their personal data is being processed.
- Access a copy of the data.
- The purpose of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or this isn't possible, the criteria to determine this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequence of this might be for the individual.

While the school will comply with the GDPR Regulations in regard to dealing with all Subject access requests submitted in any written format, individuals are asked to submit their request by letter, email or marked for the attention of the Data Protection Officer.

They should include:

- Name of individual
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If staff received a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access request

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 their child, the child must either be unable to understand their rights and the implications of the 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 will addressed on an individual basis and a pupil's ability to understand their rights will always be judged on a case by case basis.

9.3 Responding to a subject access request

When responding to requests, we may ask the individual to provide two forms of identification from the following list:

- Passport
- Driving licence
- Utility bills with current address
- Birth/marriage certificate
- P45/P60
- Credit card or mortgage statement

- We may contact the individual via phone to confirm the request was made
- We will respond without delay and within 1 month (30 calendar days) of receipt of the request
- We will provide the information free of charge

- We will tell the individual that we will comply within 3 months of receipt of the request is complex or numerous. We will inform the individual of this as soon as possible, and explain why the extension is necessary.

We will not disclose the information if it;

- Might cause serious harm to the physical or mental health of the pupil or another individual; or
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interest; or
- Is contained in adoption or parental order records; or
- Is given to the court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act upon it, or charge a reasonable fee which would only to take 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 the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information when we are collecting their data about how we use it and process it, individuals also have the right to:

- Withdraw their consent to processing at any time, where this is the lawful basis for processing.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it in certain circumstances.
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, which might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for 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 these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10.0 Parental requests to see the educational records

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 days of a written request.

Requests should be made in writing to the Data Protection Officer, and should include:

- Name of individual
- Correspondence address
- Contact number and email address

11.0 CCTV

The school may use CCTV in various locations around the school site for security and safeguarding processes. We will adhere to the ICO's code of practice for the use of CCTV, and provide training to staff in its use.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded, with security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use, and where further information can be sort.

Any enquiries about the CCTV systems should be directed to DPO.

12.0 Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

The school will obtain a signed "using images of children" consent from parent/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

The school uses photographs:

- Within school on displays, newsletters, newspapers, prospectus and medical information.
- Outside of school by external agencies and partners such as the school photographer, local and national newspapers and local and national campaigns school may be involved with.
- Online on our school website or app.
- Assessments and Education review documents etc

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos outside of school we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13.0 Data protection by design and fault

We will put measures in place to show that we have integrated data protection into our data collection and processing activities.

These include, but are not limited to the following organisational technical measures:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- 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 regulations.
- Completing data privacy impact assessments where the schools processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies or processing tools. Advice and guidance will be sort from the DPO.

- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regular, at least annual training members of staff and governors on data protection law, this policy and any related policies and any other data protection matters. Records of attendance will be kept to record the training sessions, and ensure that all data handlers receive appropriate training.
- Termly reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school DPO and all the information we are required to share about how we use and process their personal data (via our privacy notices).
    - 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.

14.0 Data security and storage records

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

In particular our organisational and technical measures include:

- Paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain personal data which will be kept under lock and key when not in use.
- 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.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular individuals.
- Encryption software is used to protect all portable devices and removable

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due negligence and take reasonable steps to ensure it is stored securely and adequately protected.

15.0 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 also be disposed of securely, where we cannot or do not need to rectify or update it. We may use a third party to safely dispose of records on school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law, and provide a certificate of destruction. A record of destruction will be kept on our systems.

16.0 Personal data breach

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 the school Breach Management procedure.

Where appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in school context may include, but are not limited to:

- A non-atomised data set being published on the school website which shows the exam results of pupils eligible for the pupil premium funding.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils or staff.

17.0 Breach Management Procedure.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidently or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people.

The DPO will alert the Headteacher and the Chair of Governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (Actions relevant to specific data types are set out at the end of this policy).

The DPO will assess whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identity theft or fraud
- Unauthorised reversal of pseudonymisation (for example key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned
- If it is likely there will be a risk to people's rights and freedoms, the DPO must notify the ICO

The DPO will document the decisions (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Breach Management Record.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned.
    - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - 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.

If all of the above are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reason why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- 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 – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause.
- Impact
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
- Records of all breaches will be stored in the Breach Management Record.

The DPO and 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.

Actions to minimise the impact of data breaches
We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after the data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If a special category data (sensitive information) is accidently made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT contractor to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who receive the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will carry out an internet search to check that the information has not been made public, if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

18.0 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work they carry out. As previously stated this policy will be reviewed after one year, and then after that point it will be reviewed every two years. The school governors will be included as part of the review process.

19.0 Data Retention

The school will adhere to statutory guidance relating to the retention of personal data.

The school will adhere to the operational guidance provided by the Information Records Management Society.

The school keeps an electronic back up of the computer systems. Back-up data may be retained in a format for a longer period that recommended by the

Information Records Management Society. This is unavoidable given the finite resources of the organisation.

20.0 Privacy Notices

Tickhill Estfeld Primary School has a Privacy Notice for the following groups of Data Subject:

- Pupils and Parents
- School Workforce
- Contacts
- Governors
- Visitors
- Volunteers

outlining:

- The legal basis on which we collect and process personal data and what we use the data for
- The categories of personal data that we collect and process
- Details of who we share personal data with
- The length of time that we retain personal data

The Privacy Notice makes explicit an individual's rights under GDPR

The Privacy Notice provides contact details for all enquiries relating to Data Protection in school

Any documentation where we collect personal data from individuals will contact a reference that clearly signposts the Privacy Notice.

Date approved	01/09/2026
Review date	01/09/2027
Headteacher	A Painter