Data Protection Policy

Yew Tree Farm School
Bredgar and Wormshill Light Railway
Swanton Street
Sittingbourne
ME9 8AT

Date - 23/01/25
Reviewed by - Executive Board
Next review date - 23/01/26

Aims

Yew Tree Farm School takes data protection very seriously. As such, this policy outlines the measures the school will put in place to ensure the protection of all personal and sensitive data about staff, governors, visitors, pupils and other individuals.

This policy outlines a data protection by design culture within the school so that all collection, storage and processing of data, whether digital or on paper, is carried out lawfully in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018

Legislation and Guidance

General Data Protection Regulation (GDPR) came into force in May 2018 as part of the Data Protection Act 2018 (DPA 2018) which replaces the previous Data Protection Act 1998. GDPR relates to the collection, processing and storage of personal data. This policy is based on guidance published by the Information Commissioner's Office (ICO) and the ICO's code of practice for subject access requests.

Definitions

Throughout this policy, the following terminology with the accompanying definitions will be used.
Terminology Definition

Terminology	Definition
processing	Any action or operation performed on personal data, such as, collecting, recording, storing, altering, using, transmitting, destroying or erasing. Processing also includes transferring personal data to third parties.
data subject	Any person about whom we hold personal data. In the case of the school this could relate to pupils, parents, staff, governors, volunteers and visitors.
personal data	Any information that relates to an identified or identifiable (either directly or indirectly), person or data subject.
sensitive data	Relates to a set of special categories that should be treated with extra security. These categories are: ● Racial or Ethnic Origin Data ● Political Opinions ● Religious or Philosophical Beliefs ● Trade Union Membership ● Genetic Data ● Biometric Data
data controller	Any person, agency or authority who decides how and why data is processed. In the case of this policy the school is the data controller.

data processor	Any person, agency or authority that processes data on behalf of a data controller.
data protection officer (DPO)	The person responsible for independent and impartial monitoring and application of laws that protect personal data within the school.
data breach	A breach of security that leads to the accidental or unlawful loss, destruction. alteration, disclosure of or access to personal data while stored, transmitted or being processed must be reported to the Information Commissioner's Office (ICO)
Information Commissioner's Office (ICO)	A UK based organisation responsible for upholding information rights.
data users	Those who process personal data. They must protect data in accordance with this data protection policy.
data	Information which is stored electronically, on a computer, or in certain paper- based filing systems.
biometric data	Personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints

Roles and Responsibilities

Yew Tree Farm School will follow the outline below for distribution of responsibilities in relation to GDPR within the school.

Role	Responsibility
Governing Body	The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.
Headteacher	The headteacher acts as the representative of the data controller on a day-to-day basis.
Data Protection Officer (DPO)	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, procedures and guidelines where applicable.

	The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Our DPO is Olivia Williams and contactable on office@yewtreefarmschool.co.uk or 07493097080.
All other Staff ie 1-1's, Office staff	All 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

Data Protection Principles

The data protection principles that the school must follow in order to be compliant with GDPR state that personal data
must be:

- processed lawfully, fairly and in a transparent manner;
- collected for legitimate purposes;
- relevant and limited to what is necessary in order to fulfill the purposes for which it is processed;
- kept up to date;
- stored for no longer than is necessary;
- processed in a way that ensures it is appropriately secure.

This policy outlines how the school will comply with these principles.

Collecting Personal Data

Collecting personal data will be an inevitable part of the day-to-day business of Yew Tree Farm School. We will only collect personal data for specific, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. To ensure that this data is handled and processed appropriately and with minimal risk, Yew Tree Farm School as data controller, adheres to the guidelines outlined below.

Scenario	Procedure
Pupil Contact Records	Stored securely on Google drive (individual usernames and passwords) and CPOMs (multi-factor authentication code log in each time), also paper copy filed away in a secure filing system.
Pupil Attendance Records	Stored on CPOMs with multi-factor authentication code log in
Pupil Progress Data	Reported on Tapestry and Google Drive with individual usernames and passwords
Staff Records	Stored securely on Google drive account with individual usernames and passwords
Special Educational Needs (SEN) Records	Stored securely on Google drive, CPOMs and paper copies in secure filing cabinet
Medical Information and Administration	Stored on CPOMs with multi-factor authentication code log in
Safeguarding Records	Stored on CPOMs with multi-factor authentication code log in

Sharing Personal Data

As with the collection of personal data, it is integral to the effective functioning of Yew Tree Farm School that personal data will need to be shared in certain circumstances. To ensure that personal data is shared lawfully, the following considerations must be taken into account.

Scenario	Procedure
Regulatory Bodies e.g. government agencies or healthcare	Before sharing personal data with regulatory bodies requesting access, the DPO will verify the identity of the body and investigate how they intend to use the data shared with them. Only when satisfied with the response will Yew Tree Farm School share any personal data.
Suppliers or Subcontractors Requiring Access to Personal Data	The DPO will assess all suppliers and subcontractors' ability to adhere to GDPR. All suppliers and subcontractors requiring access to personal data will read and follow the school GDPR policy.
The Police	The police will only be able to request access to data with a relevant warrant.

Subject Access Request (SAR)

As part of GDPR, data subjects are entitled to make a request to any organisation, such as a school, to access personal data held about them. This is known as a subject access request (SAR). Yew Tree Farm School

therefore needs to be reasonably prepared for such an eventuality by establishing the procedure outlined below.
NB: Personal or sensitive data about a child belongs to the child. However, if a child is deemed unable to understand their rights or the implications of a SAR, or is unable to give consent, a parent or guardian can make the request on their behalf.

Subject Access Request Procedure

1) All staff are trained to recognise a subject access request.
2) Staff involved in responding to a SAR clearly understand the notion of the right to access. They also know when a SAR can be refused and how to act when refusing a SAR.
3) The school will use the school specific SAR form. (See appendix 1)
4) Identification of the subject requesting access will be verified.
5) The school aims to respond to all SARs within one month of submission.
6) Upon receiving a valid SAR, the following procedure will be followed:
    - The staff member who receives the written SAR refers this to the headteacher (or another member of senior leadership team if necessary).
    - A review of the SAR is carried out in order to establish the exact information requested.
    - The SAR is recorded in the school SAR log and reported to the DPO.
    - The DPO will send a response to the data subject to inform them that their SAR is being processed.
    - The information will be collated and the request responded to.
    - The record on the SAR log is marked as closed.

Photos, Video, CCTV

Yew Tree Farm recognises that photos, videos and CCTV images of individuals will be part of the personal data processed by the school. As a result, the following measures are adhered to in order to ensure responsible handling and processing of such data.

- Photos and videos taken within school for public use are to be considered under GDPR.
- Any photo or video of recognisable individuals which the school wishes to publish for example, on the school webpage or social media platform, will only be published with prior written consent. Written consent will be obtained via completion of [include relevant school document].
- Photographs and video captured by parents for personal use do not fall under the scope of GDPR.

Data Retention - Security and Storage

At Yew Tree Farm School only data that is adequate, purposeful, necessary and limited to what is essential will be stored. The school will ensure that any stored data will be protected from unauthorised access and data breaches through the implementation of up to date and well-maintained security protocols. This will guarantee the confidentiality, integrity and availability of personal data. Confidentiality means that data will only be accessed by those who are authorised to access it. The integrity will be maintained through guaranteed accuracy and suitability of all data stored; inaccurate or unsuitable data will not be retained. Availability will be maintained, meaning those that are authorised to access the personal data are able to do so as and when required.
Student data, (Names, Address, Contact Details etc.) will be kept for a period of 1 year after the student leaves Yew Tree Farm School for dispute resolution (and any other purposes) etc, after which it will be purged from record at the next annual review cycle.

Specific Data Types	Security Measures
paper records	All paper records stored on site will be kept in a secure and locked location. Only those authorised to access the records will be granted access to the storage location.
portable electronic devices e.g. Laptops, iPads.	All portable electronic devices will be password protected. In the case of laptops the hard drives will be encrypted.
papers containing personal data e.g. class lists contact sheets dinner registers	Any paperwork containing personal data will not be left unattended and in sight at any time. Teachers and other classroom staff will ensure that any paper containing personal data will be suitably stored to limit access to the data.
desktop computers within the school	All computers used in the school will be password protected and have a timed lock function when left unattended. Staff will be required to lock their workstations when leaving them unattended at any time.
staff personal devices	Staff will not be permitted to use personal devices to access or store any personal data relating to the school.
sharing with authorised third parties	When required to share data with authorised third parties, the school and staff will make the necessary checks to guarantee it is handled securely and in line with GDPR.

Biometric Data

Yew Tree Farm School does not use Biometric Data in any form and has no need for it.
Biometric data is personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints.

'Processing' of biometric data includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- recording pupil/students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner
- storing pupil/students' biometric information on a database system
- using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupil/students'

It is the responsibility of the data controller to identify the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented. Controllers should also, be

aware of the wider duties placed on them, for example under the Human Rights Act 1998 and Public Sector Equality Act Duty using automated biometric technology. Controllers should also consult with the ICO when making these decisions.

Purpose - In line with the purpose limitation principle under Data Protection law, schools and colleges can only store and use the biometric information for the purpose for which it was originally obtained and parental/child consent given.

Security - We would expect schools and colleges to carry out the following when considering security of biometric data:

- store biometric data securely to prevent any unauthorised or unlawful use
- not keep biometric data for longer than it is needed meaning that a school or college should destroy a pupil's/student's biometric data if, for whatever reason, they no longer use the system including when leaving the school or college, where a parent withdraws consent or the pupil/student either objects or withdraws consent
- ensure that biometric data is used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties.

Data Controller Responsibilities

It is the responsibility of the data controller to identify the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented. Controllers should also, to be aware of the wider duties placed on them, for example under the Human Rights Act 1998 and Public Sector Equality Act Duty using automated biometric technology. Controllers should also consult with the ICO when making these decisions.

Protection against unlawful and unauthorised access - It is important that schools and colleges understand their responsibilities, when protecting data. Schools and colleges should:

- identify risks that emerge from the initial assessment
- assess what can be done to eliminate or reduce areas of medium/high risk and set action plans to do so
- consider access controls
- use DPIAs as a part of their risk identification and mitigation procedures ensuring that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented. This will include third party providers of any technology used.

Staff Remote Working

For remote working to comply with GDPR, Yew Tree Farm School implements the following procedures:

- All staff laptops will have encrypted hard drives and will be password protected.
- When working remotely and accessing the school network, staff will use a secure password; this will prevent unauthorised access to school computer systems and networks.
- Staff will only be able to use electronic devices provided by the school to work at home on any personal/sensitive data and/or access the school network.
- Staff laptops will have up-to-date antivirus software installed to prevent any malicious or unauthorised access to school records, personal or sensitive data.
- Staff are permitted to use personal or home Wi-Fi networks but are not permitted to use public Wi-Fi when working remotely. Public Wi-Fi security is not always strong enough to prevent a data breach.

- All laptops provided by school will be encrypted and password protected. If using a USB stick to transport personal or sensitive data, this will also be encrypted.
- All staff will use Kensington Locks when using a laptop to work at home.

Disposal of Data

Yew Tree Farm School will always ensure that records containing personal and/or sensitive data are disposed of safely and securely.
For example, any paper records due to be disposed of will be securely shredded, either on site, or through an approved third-party disposal service. When using a third party, it is the school's responsibility to ensure that the company guarantees the records are disposed of securely.
Any digital records containing personal data will be deleted using the internal erasure procedure of the relevant software. For example, records stored on a Windows laptop would be deleted using the Windows secure delete functions. It is up to individuals to make sure they have deleted personal data from devices once that data is no longer relevant, or the device is being passed on. When disposing of sensitive personal data, the school will use a file-wiping utility to remove the sensitive personal data, preventing the possible retrieval if erased, using internal procedures

Compliance Monitoring

As data collection and processing changes and updates, Yew Tree Farm School confirms continual compliance through compliance monitoring. The designated DPO will, as part of their role, undertake regular monitoring of data records held by the school, checking they are relevant, necessary and accurate. The DPO will monitor the compliance of the roles outlined in this policy with their assigned responsibilities, impartially checking that these are carried out in accordance with policy. The DPO will monitor who the school is sharing data with and the integrity and necessity of the third-party data processing. The DPO will monitor procedures for SAR and data breaches, ensuring these are followed correctly and in a timely manner.

Data Breaches

At Yew Tree Farm School all reasonable action will be taken to keep data handling and processing safe and secure within GDPR. However, should a data breach occur, Yew Tree Farm School will be prepared to handle any such breach in the manner outlined below. Potential data breaches within a school context could be the loss of a USB containing pupil assessment data or an email containing sensitive personal data could be sent to an incorrect email address.

Yew Tree Farm School Procedure for Handling A Data Breach

- Any potential or confirmed data breach must be reported in the first instance to the DPO.
- Upon receiving notification of a data breach, the DPO must report this to the headteacher and chair of governors.
- The DPO will investigate the data breach further to assess the severity of the breach.
- Once the assessment has been made the outcome will be logged by the DPO, whether the breach does or does not need reporting. The log will include the cause of the data breach and any facts surrounding the breach, the effects of the breach and the action taken to minimise risk and prevent a repeat occurrence.
- If the DPO determines that the data breach poses a significant threat to the data subject(s), they will report the breach to the ICO within 72 hours.

- The DPO will attempt to minimise the impact of the breach, supported by relevant parties within the school.
- Upon receiving the ICO report, the DPO will act upon the ICO's recommendation.

Training

To guarantee continued compliance with GDPR all staff will receive data protection training as part of the induction process at Yew Tree Farm School. Staff will receive training annually for GDPR and their responsibilities within keeping data protection safe. Ongoing continuing professional development (CPD) for all staff will include relevant and topical GDPR training.

GDPR Training Log

Date	Who	Training Description
28/09/23	Olivia Williams	GDPR in Education Training

Links to Other Policies

The following policies should be read and considered in conjunction with this GDPR policy:

- Assessment Policy
- Privacy Policy
- Safeguarding Policy

Appendix 1
Yew Tree Farm School

Subject Access Request Form	
Title	
Surname	
First Name(s)	
Date of Birth	
Home Address	
Post Code	
Contact Telephone Number	
Email Address	
Relationship with the school	
Identification provided To validate name and address	
Details of data request Please include as much information as possible about the data you are requesting. For example: your personal file, your child's progress data, emails sent between A and B and specific dates.	

I am requesting access to my own personal data, as detailed above. I confirm that I am the individual named above and the data I am requesting access to is my own personal data. I have supplied the information above to aid the subject access request and also to validate my identity. I have provided identification to prove my name and address.

Signature _____ **Date** _____

Appendix 2
Yew Tree Farm School

Data Breach Log Form	
Date of breach	
Date of breach discovered	
Cause of breach	
Description of the breach What happened? Who is involved? Other facts:	
Reported to ICO?	
Date reported to ICO (If reported)	
All data subjects informed?	
Remedial action	
Follow-up (if required)	
Breach reported by	
Date reported	
Report received by	