DATA PROTECTION POLICY (including GDPR)

The Board of Trustees, CEO and Strategic team are committed to safeguarding and promoting the welfare of children and young people and requires all staff and volunteers to demonstrate this commitment in every aspect of their work.

This policy was created and ratified by the Wensum Trust Board:	**November 2020**
Responsible person for updating:	**Director of Operations**
This policy will be reviewed by the Wensum Trust Board: **(unless earlier review is recommended by the Wensum Trust)**	**November 2022**
Policy Version:	**V1.3**
Signed by the Chair of the Board of Trustees:	

Associated Documentation

Guide to GDPR provided by Gov.uk

Related Policies

- ICT/E-Safety Policy
- Retention Schedule
- Safeguarding Policy

Contents

1. Definitions

- The Trust means The Wensum Trust
- Principal/Headteacher refers to Principals at Secondary Phase and Headteacher at Primary Phase
- Governor also means Trustee depending on reporting channels
- DPO means the Data Protection Officer, which is an external provider to the Trust
- Establishment means Academies of the Trust, Central Service Office and any other site under the control of the Trust
- Governing Board means Trust Board, Committees of the Trust Board and/or Local Advisory Board depending upon delegation from Trustees
- Staff means any person employed by the Trust across its establishments

2. Aims

The Trust and all the establishments within the trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors 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.

3. 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 Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to the Trust's use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and 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's educational record.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's:

	• Name (including initials) • Identification number • Location data • Online identifier, 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 accidental or unlawful destruction, loss, alteration,

	unauthorised disclosure of, or access to personal data.

5. The Data Controller

The Trust and all the establishments within the trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore each establishment gathering data is deemed to be the data controller.

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

6. Roles and Responsibilities

This policy applies to **all staff** employed across The Trust, and to external organisations or individuals working on the Trust's behalf. Staff who do not comply with this policy may face disciplinary action.

6.1. Local Advisory Board / Board of Trustees

The local advisory board for each school and the Wensum Trust board of trustees have overall responsibility for ensuring that the academy in case of the Local Advisory Board and the Trust Office Headquarters in case of the Board of Trustees comply with all relevant data protection obligations.

6.2. Data Protection Officer

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 and guidelines where applicable.

They will provide an annual report of their activities directly to the relevant governing board and, where relevant, report to the board their advice and recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Data Protection Education Ltd. and is contactable via dpo@dataprotectioneducation.

6.3. Headteacher / Principal

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

6.4. All Staff

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 European Economic Area
- 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

7. 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
- Must not be transferred to people of organisations situated in other countries without adequate protection

This policy sets out how the Trust and its establishments aim to comply with these principles.

8. Collecting Personal Data

10.3. Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- 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
- 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 e.g. 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 functions
- 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)
- 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 processing which are set out in the GDPR and 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 parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

10.4. Limitation, 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 Wensum Trust's retention schedule.

9. Sharing Personal Data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - 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
    - Only share data that the supplier or contractor needs to carry out their service, 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, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided
- The interests of public health, including NHS Test and Trace

We may also share personal data with emergency services and local authorities to help them to 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.

A Privacy Notice for students / parents and staff is shared at the start of each academic year, which sets out the purpose or collecting personal data and the lawful basis for any processing.

10. Subject Access Requests and other Rights of Individuals

10.5. 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:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes 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 if this isn't possible, the criteria used 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 consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

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

10.6. 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 their 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 aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil if they are aged 12 and above. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.7. Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- 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
- Is contained in adoption or parental order records
- 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 the right to complain to the ICO.

10.8. 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:

- Right to fair and transparent processing
- Right of access

- Right of rectification
- Right to erasure (the 'right to be forgotten')
- Right to restrict processing
- Right to be notified of erasure, rectification or restriction
- Right of data portability
- Right to object to processing
- Right to object to processing for scientific, historical or statistical purposes
- Right to not be evaluated on the basis of automated processing
- Right to withdraw consent at any time
- Right to be notified about a data breach
- Right to be an effective judicial remedy again a supervisory authority
- Right to lodge a complaint with supervisory authority
- Right to an effective judicial remedy against a controller or processor
- Right to compensation

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 / Director of Data.

11. Parental Requests to see the Educational Record

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

There is no automatic parental right of access to the educational record for academies, including free schools. Please contact the DPO for further information and how a request can be made.

12. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can be given a code to use rather than using the biometric system(s).

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

13. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to Mr R Marrison, Estates Manager for the Wensum Trust.

14. Photographs and Videos

As part of the Trust and its establishments activities, we may take photographs and record images of individuals within each establishment.

We will obtain written consent from parents/carers, or pupils aged 18 and over (in accordance with safeguarding procedures), for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- On internal notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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 in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

15. Audio Recordings

As part of the Trust and its establishments activities, we may take audio recordings within each establishment.

We will obtain written consent from parents/carers, or pupils aged 18 and over (in accordance with safeguarding procedures), for audio recordings to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the audio recording will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the audio recording will be used.

Uses may include:

- Outside of school by external agencies such as newspapers, campaigns etc
- Online on the Trust or its establishments website or social media pages

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

When using audio recordings in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

For other recordings please see relevant policies, such as Complaints Policy.

16. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of the Trust's data processing activities, including:

- 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 law (see section 6)
- Completing privacy impact assessments where the establishment's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- 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
- Regularly conducting 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 the establishment and DPO and all 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

17. 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:

- 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
- 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
- Where personal information needs to be taken off site, staff must sign it in and out from the relevant establishment
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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 (see our ICT / e-safety policy and acceptable use policy)
- 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)

18. 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.

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

19. Personal Data Breaches

The Trust and its establishments 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 an establishment context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a laptop belonging to the Trust or its establishments containing non-encrypted personal data about pupils

20. 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 Trust or its establishments processes make it necessary.

21. Monitoring and Review of Policy

The Trust will review this policy every 2 years and assess its effectiveness and implementation. Any deficiencies identified shall be corrected and used to inform review of the policy, which will be promoted and implemented throughout the Trust.

The Director of Operations & Finance with input for the DPO will report on the effectiveness of the policy to the Trust Board/ relevant committee as appropriate.