



Data Protection Policy

(inc. Privacy Notices, and Covid-19
Mass Testing Privacy Notice)

Category:	Data Protection	
Authorised By:	Audit and Risk Committee	
Author:	S. Urding & WES Legal Services	
Version	3	
Status:	Under Review:	
	Approved:	✓
	Adopted:	✓
Issue Date:	October 2021	
Next Review Date:	October 2022	
Statutory Policy:	Yes	✓
	No	

Contents

<u>Section</u>	<u>Page</u>
1. Scope	3
2. Policy Statement	3
3. Principles	4
4. Definition of Terms	4
5. Procedure	5
6. Equality Statement	11
7. Monitoring of Policy	11
Appendices	12
1. Personal Data Breach Procedure	15
2. Additional Guidance for Staff	16
3. Checklist for obtaining consent	17
4. Privacy Notice for parents/carers	22
5. Privacy Notice for pupils/students	27
6. Privacy Notice for staff	31

1 – Scope

1.1 This policy applies to **all staff** employed by TLET, and to external organisations or individuals working on our behalf. It aims to outline guidance and procedures in the management and control of paper based and electronic data.

1.2 **Board of Trustees**

The Board of Trustees has overall responsibility for ensuring that the Trust and its academies comply with all relevant data protection obligations.

1.3 **Data Protection Officer (DPO)**

The DPO is the first point of contact for individuals whose data the Trust and its academies process, and for the Information Commissioner’s Officer (ICO).

1.4 The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

1.5 The GDPR does not include a specific list of DPO credentials, but Article 37 does require a DPO to have “expert knowledge of data protection law and practices.” For this reason, the Trust’s DPO is the DPO at Warwickshire Education Service (WES) and is contactable via schooldpo@warwickshire.gov.uk

1.6 The Trust processes personal data relating to parents, pupils/students, staff, partners, trustees, visitors and others, and therefore is a data controller.

1.7 Transforming Lives Educational Trust and its academies are registered as data controllers with the ICO and will renew this registration annually or as otherwise legally required.

1.8 **Principal**

The Principal acts as the representative of the data controller on a day-to-day basis in each Trust academy. The CEO acts as the representative within the Central Team.

1.9 **All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the academy 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

2 – Policy Statement

2.1 The Transforming Lives Educational Trust (the Trust) aims to ensure that all personal data collected about staff, pupils/students, parents, partners, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

2.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3 – Principles

- 3.1 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.
- 3.2 It meets the requirements of the Protection of Freedoms Act 2012 when referring to the Trust’s use of biometric data.
- 3.3 It also reflects the ICO’s code of practice for the use of surveillance cameras and personal information.
- 3.4 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.
- 3.5 In addition, this policy complies with our funding agreement and articles of association.
- 3.6 The GDPR is based on data protection principles with which the Trust and its academies must comply. The principles state 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
- 3.7 This policy sets out how the Trust aims to comply with these principles.

4 – Definition of Terms

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual. This may include the individual’s:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual’s:</p> <ul style="list-style-type: none">• Racial or ethnic origin• Political opinions• Religious or philosophical beliefs• Trade union membership

	<ul style="list-style-type: none"> • 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 – Procedure

5.1 Collecting personal data

5.1.1 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:

1. The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
2. The data needs to be processed so that the Trust can **comply with a legal obligation**
3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone’s life
4. The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest**, and carry out its official functions
5. The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual’s rights and freedoms are not overridden)
6. The individual (or their parent/carer when appropriate in the case of a pupil/student) has freely given clear informed **consent**

5.1.2 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.

5.1.3 If we offer online services to pupils/students, such as classroom apps, and we intend to rely on use consent as a basis for processing, we will get parental consent where the pupil/student is under 13 (except for online counselling and preventive services).

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

5.1.5 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.

5.1.6 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.

5.1.7 Staff must only process personal data where it is necessary in order to do their jobs.

5.1.8 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

5.2 Sharing personal data

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

- There is an issue with a pupil/student 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/students – 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

5.2.2 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

5.2.3 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/students or staff.

5.2.4 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.

5.3 Subject access requests and other rights of individuals

5.3.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust and its academies hold 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
- 5.3.2 The Trust encourages the practice that Subject Access Requests be submitted in writing by letter, email or fax to the Principal of each Trust academy. They should include:
- Name of individual
 - Correspondence address
 - Contact number and email address
 - Details of the information requested
- 5.3.3 If staff receive a subject access request they must immediately forward it to the Principal.
- 5.3.4 **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.
- 5.3.5 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, most subject access requests from parents or carers of pupils/students attending one of our academies may not be granted without the express permission of the pupil/student. This is not a rule and a pupil's/student's ability to understand their rights will always be judged on a case-by-case basis.
- 5.3.6 **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
- 5.3.7 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
- 5.3.8 **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 5.9), individuals also have the right to:

- Withdraw their consent to processing at any time
- 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, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

5.3.9 Individuals should submit any request to exercise these rights to the Principal. If staff receive such a request, they must immediately forward it to the Principal.

5.4 Parental requests to see the educational record

5.4.1 As an academy trust there is no automatic parental right of access to the educational record. However, where possible we will seek to accommodate parental right of access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

5.5 Biometric recognition systems

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

5.5.2 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.

5.5.3 Parents/carers and pupils have the right to choose not to use the school's biometric system(s).

5.5.4 We will provide alternative means of accessing the relevant services for those pupils/students.

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

5.5.6 As required by law, if a pupil/student 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/student's parent(s)/carer(s).

5.5.7 Where staff members or other adults use the academy'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.

5.6 CCTV

5.6.1 We use CCTV in various locations around the Trust's academy sites to ensure they all individuals remains safe.

5.6.2 We will adhere to the ICO's code of practice for the use of CCTV.

- 5.6.3 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.
- 5.6.4 Any enquiries about the CCTV system should be directed to the Principal.

5.7. Photographs and videos

- 5.7.1 As part of our Trust activities, we may take photographs and record images of individuals within our academies.
- 5.7.2 We will obtain written consent from parents/carers, or students aged 13 and over, for photographs and videos to be taken of pupils/students for communication, marketing and promotional materials.
- 5.7.3 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/student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.
- 5.7.4 Uses may include:
- Within academies on notice boards and in academy magazines, brochures, newsletters, SIMS etc.
 - Outside of academies by external agencies such as the academy's photographer, newspapers, campaigns
 - Online on our Trust and academy websites
- 5.7.5 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.
- 5.7.6 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.

5.8 Data protection by design and default

- 5.8.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
- Subscribing to Warwickshire Educational Services which offer a suitably qualified DPO service
 - 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
 - Completing impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
 - Integrating data protection into internal documents
 - Regularly training members of staff on data protection
 - 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 our academies and all information we are required to share about how we use and process their personal data (via our Privacy Notices – see Appendix 4, 5 and 6)
 - 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

5.9 Data security and storage of records

5.9.1 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.

5.9.2 In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure 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 gain permission and ensure its security at all times (for example through encrypted password protection)
- Passwords that are at least 8 characters long containing letters and numbers are used to access academy computers, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as USB or other portable devices
- Staff, pupils/students, partners or trustees who store personal information about others on their personal devices are expected to follow the same security procedures as for academy-owned equipment
- 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

6.0 Disposal of records

6.0.1 Personal data that is no longer needed will be disposed of securely.

6.0.2 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.

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

6.1 Personal data breaches

6.1.1 The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

6.1.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

6.1.3 When appropriate, we will report the data breach to the ICO within 72 hours.

6.1.4 Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the Trust and/or academy website which shows the exam results or destinations of pupils/students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft or loss of an academy laptop or electronic data storage device containing non-encrypted personal data about pupils/students

6.2 Training

6.2.1 All staff, partners and trustees are provided with data protection training as part of their induction process.

6.2.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the academy's processes make it necessary.

6 – Equality Statement

- 6.1 This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any individual (with due regard to their protected characteristics), and it helps to promote equality across the Trust.

7 – Monitoring

- 7.1 It is the responsibility of the Board of Trustees, and those they delegate authority, to ensure that the principles and procedures of this policy are adhered to. The use of this policy will be subject to routine monitoring to ensure its fidelity in practice. The evidence gathered from monitoring at regular intervals shall inform any reviews and future revisions to the policy, and no later than that stated on Page 1 of this policy.

Appendix 1: Personal Data Breach Procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Principal/CEO.
- The Principal/CEO will notify the DPO immediately and then, under their direction, investigate the report and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people third parties
- The Principal/CEO will alert the DPO, Chair of AIM Board and the Chair of Trustees.
- The Principal/CEO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members, DPO or data processors where necessary.
- The Principal/CEO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The Principal/CEO will, in consultation with the DPO, determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Principal/CEO 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
 - Identify theft or fraud
 - Financial loss
 - 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 that there will be a risk to people's rights and freedoms, the Principal must notify the ICO.

- The Principal/CEO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- 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 the above details 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 reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Principal 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 and Principal
 - 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(s) concerned
- The Principal will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The Principal will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The DPO and Principal will 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 any data breach.

Sensitive information being disclosed via email (including safeguarding records) could include but is not limited to:

- *If special category data (sensitive information) is accidentally 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 Principal will ask IT Services to recall it*
- *In any cases where the recall is unsuccessful, the Principal will contact the relevant unauthorised individuals who received 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 Principal will ensure those individuals concerned receive a written response from all the individuals those who received the data, confirming that they have complied with this request*
- *The Principal will carry out undertake 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*

Other types of breach could include, but is not limited to:

- *Details of pupil premium interventions for named children being published on the academy's website*
- *Non-anonymised pupil exam results or staff pay information being shared with Aim partners and/or trustees*
- *A school laptop or other electronic data storage device containing non-encrypted sensitive personal data being stolen, lost or hacked*
- *The academy's cashless payment provider being hacked and parents' financial details stolen*

Complaints

Complaints about the above procedures should be made to the academy's Chair of AIM Board who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Trust's complaint procedure.

Complaints which are not appropriate to be dealt with through the Trust's complaints procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact the Principal.

Appendix 2: Additional Guidance for Staff

These guidelines represent the latest information and guidance and are subject to updates

- Staff should familiarise themselves with the contents of this policy and ensure they comply with the General Data Protection Regulations
- Staff should not remove any 'personal' or 'sensitive' data from the academy if at all possible, the preferred method of access being remotely via a secure connection


Article 4 (1) of GDPR defines personal data as being:

- *'Any information relating to an identified or identifiable natural person' ('data subject');*
- *'An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'*

This now includes IP addresses, biometric data, mobile device ID's, cookies on websites.

- Any electronic use of this type of personal or sensitive data should be strictly limited to whole academy analysis by authorised staff only.
- If personal and sensitive data is removed electronically, then it is encrypted – encrypted memory sticks are available from IT Services.
- 'Day to day data' such as electronic mark books and assessment data does constitute personal and sensitive information and should still be kept securely against theft or loss. The individual being mindful of how this data could be used in conjunction with other data.
- This data should not be transferred to the hard disk of home computers / laptops.
- Measures should be taken to ensure the security of devices, which contain personal data when not in academies.
- If data is lost then it should be reported immediately to the Principal.
- Any communication/transfer of data to a third party should only take place with written parental consent.
- The capture and use of pupil/student-photographs should be limited and parental permission received.
- Parents should be informed of how we collect, use and safeguard student data.
- Parents should be informed of all data which is held on their children, its use, its life-span and the potential risk involved and how the school mediates against that risk – this is communicated via the Privacy Statement issued to parents and available on the Trust's academy websites.
- Every member of staff should be informed of what data is held on them by the Trust, why, for what purpose, how long it will be kept and how it is safeguarded.

Appendix 3: Checklist for obtaining consent under the GDPR

Action	
Asking for consent	
We have checked that consent is the most appropriate lawful basis for processing	
We have made the request for consent prominent and separate from other terms and conditions	
We ask people to positively opt in	
We don't use pre-ticked boxes, or any other type of consent by default	
We use clear, plain language that is easy to understand	
We specify why we want the data and what we're going to do with it	
We have named our organisation and any third parties	
We tell individuals they can withdraw their consent and we don't make consent a pre-condition of a service	
We ensure that the individual can refuse to consent without detriment	
Recording consent	
We keep a record of when and how we got consent from the individual and what they were told at the time	
Managing consent on an on-going basis	
We regularly review consents to check that the relationship, the processing and the purposes have not changed	
We have processes in place to refresh consent at appropriate intervals, including any parental consents	
We make it easy for individuals to withdraw their consent at any time, and publicise how to do so	
We act on withdrawals of consent as soon as we can	
We don't penalise individuals who wish to withdraw consent	

Appendix 4: Privacy notice for parents and carers

Under data protection law, individuals have a right to be informed about how Transforming Lives Educational Trust and its academies use any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils/students**.

We, Transforming Lives Educational Trust, are the 'data controller' for the purposes of data protection law.

Our data protection officer is provided by Warwickshire Education Services (WES).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils/students includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil/student and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils/students that we have received from other organisations, including other schools/academies, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil/student learning
- Monitor and report on pupil/student progress
- Provide appropriate pastoral care
- Protect pupil/student welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils'/students' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

We may also process pupils'/students' personal data in situations where:

- We have obtained consent to use it in a certain way a manner which has been specified
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils'/students' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils'/students' personal data overlap, and there may be several grounds, which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils/students is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils/students while they are attending one of our academies. We may also keep it beyond their attendance at one of our academies if this is necessary in order to comply with our legal obligations.

The academy which the pupil attended until statutory school leaving age is responsible for retaining the pupil record until the pupil reaches the age of 25 years.

Data sharing

We do not share information about pupils/students with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with data protection law) we may share personal information about pupils/students with, but not limited to, the following:

Third Parties	Reason for Processing	Legal Basis	Type of Information
Warwickshire County Council / Warwickshire Educational Services	Such as safeguarding concerns, exclusions, third party service provision	Public task	Name, age, date of birth, gender, unique pupil number, address
Essex Educational Services and Evolve	To manage, process and record school visit and trip data	Consent	Name
Central and local government	Such as safeguarding concerns, exclusions, third party service provision	Public task	Name, age, date of birth, gender, unique pupil number, address
The Department for Education	Census data	Public task	Name, age, date of birth, gender, unique pupil number

Education and Skills Funding Agency	Funding	Public task	Name, age, date of birth, gender, unique pupil number, FSM
The pupil's family and representatives	Sharing progress and data, pastoral care, securing engagement, trips/visits, complaints, referrals to third party services, seek consent	Consent	Name, age, date of birth, gender, address, medical information
Pupil referral services to support learning and pastoral care	Third party service providers such as Reach/Camhs/Marf	Public task	Name, age, date of birth, gender, unique pupil number, address, medical information
Pupil records services	Third party service providers such as The Learning Records Service	Public task	Name, unique pupil number
Other educational providers such as our curriculum partner schools or services which offer alternative educational provision	Third party service providers such as Warwickshire College, Guilsborough School	Public task	Name, age, date of birth, gender, unique pupil number, medical information
Educators, examining bodies and associated data transfer systems for access arrangements and data transfers to awarding bodies	Third party service providers such as examination boards, testing organisation, awarding bodies, examination regulators and The School Performance Data Unit	Public task	Name, age, date of birth, gender, unique pupil number
Admissions	Third party service providers such as Clerks Associates who manage admission appeals	Public task	Name, age, date of birth, gender, address, medical information, photograph
Destinations data transfers	Third party service providers who monitor post-16 provision and performance	Public task	Name, age, date of birth, gender, qualification outcomes
Provision from contracted service providers	Third party service providers such as Sims, Edulink, Study Bugs and SISRA, GL Assessments	Public task	Name, age, date of birth, gender, home address, photograph; name of parent(s)/carer(s); ethnicity; unique pupil number, medical information, SEN and FSM/PP designations; assessment, behavior and attendance history

To enable provision from contracted service providers	Third party service providers such as Kerboodle; Hegarty Maths; MathsWatch; My Maths; Complete Maths; Times Table Rock Stars; GCSEPod; Wix; Viva; Educake; KUDOS, Eclipse Library Service; Prospect for careers advice and guidance	Public task	Name/ username; date of birth; name of school
Website and wireless services	Third party service providers for such as Google/Drive, Smoothwall and Meraki	Public task	Internet history
Financial organisations	Third party service providers such as BioStore (cashless system) and ParentPay	Public task	Biometric fingerprint, name, address, photograph
Our auditors	Third party service providers who audit the school's finances	Public task	Name
Health authorities	Third party service providers such as the NHS	Vital Interests	Name, address, age, date of birth, next of kin, medical information, SEN
Security organisations	Third party service providers for example for CCTV	Public task	Photograph, visual image
Health and social welfare organisations	Third party service providers to support the pastoral, medical and SEND care and provision	Public task or Vital Interests (if the individual is unable to give their consent)	Name, address, age, date of birth, next of kin, medical information
Public Health England	NHS Test and Trace	Public task	Name, date of birth, year group, parent's contact number, COVID-19 test results
Professional advisers and consultants	Third party service providers such as behaviour, attendance and counselling services	Public task	Name, SEN and FSM information,
Police forces, courts, tribunals	Third party legal or regulatory organisations	Public task	Name, address, age, date of birth, next of kin, medical information, SEN, FSM
Colleges and Universities	Post-16 provision, for example university open day visits or interviews	Public task	Name, address, age, date of birth, qualification outcomes

Tour operators for trips and visits	Third party service providers to enable trips and school visits to occur, for example PGL, Rayburn Tours, World Challenge	Consent	Name, address, age,
Work experience placement organisations	For example where references are required or where a work experience placement is being organised	Public task	Name, address, age, medical, SEN
Emailing and texting services to communicate with parents	Third party service providers such as Click Send and Google Guardian	Public task	Name, phone number, email address

National Pupil/Student Database

We are required to provide information about pupils/students to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools/academies, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations, which promote children’s education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department’s webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

Youth support services

Once our pupils/students reach the age of 13, we are legally required to pass on certain information about them to Warwickshire County Council and other third-party youth support services as it has legal responsibilities regarding the education or training of 13-19-year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils/students once aged 16 or over, can contact our Data Protection Officer to request that we only pass the individual’s name, address and date of birth to Warwickshire County Council and other third-party youth support services.

Transferring data internationally

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.

Parents and pupils’/students’ rights regarding personal data

Individuals have a right to make a ‘**subject access request**’ to gain access to personal information that the Trust or its academies hold about them.

Parents/carers can make a request with respect to their child’s data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the Trust or its academies holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it

- Tell you why we are holding and processing it, and how long we will keep it for
- Explain from where it originated, if not from you or your child
- Tell you with whom it has been, or will be, shared
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would wish like to make a request then you should contact the Principal of the academy your child attends. Parents/carers also do not have an automatic legal right to access to their child's **educational record** as your child/ren attend an academy. However, wherever possible we support parents'/carers' request to access their child's educational record. To request access, please contact your child's Principal.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please parents/carers should contact the Principal of the academy your child attends.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact Complaints should be made in the first instance to the the Principal of the academy your child attends. Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact your child's Principal.

Appendix 5 - Privacy notice for pupils/students

You have a legal right to be informed about how our Trust and its academies use any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.

We, Transforming Lives Educational Trust are the 'data controller' for the purposes of data protection law.

We commission Warwickshire Educational Services (WES) for data protection advice, guidance and compliance.

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at your academy.

For the same reasons, we get information about you from some other places too – like other schools/academies, the local council and the government.

This information includes, but is not limited to:

- Your contact details
- Your family details
- Whether your family is eligible for financial assistance (for example Pupil Premium Funding and Free School Meals)
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions (past or present)
- Photographs
- CCTV images

Why we use this data

We use this data to help run the Trust and its academies, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you need any extra help
- Track how well the Trust and its academies are performing
- Look after your well-being and safety and the well-being and safety of others
- Ensure that our policies and practices are adhered to
- Meet our legal and legitimate obligations as a school and educational provider
- Offer you services through third party providers (such as access to the internet, sharing your details with examination boards and offering you educational visits and trips)

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)
- Fulfil our legitimate function as an academy and educational provider

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else’s interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds, which mean we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it’s optional. If you must provide the data, we will explain what might happen if you don’t.

How we store this data

We will keep personal information about you while you are a pupil/student at one of our academies. We may also keep it after you have left the Trust, where we are required to by law or where you may request us to write a reference to a prospective employer.

The school/academy, which the pupil/student attended until statutory school leaving age 7, is responsible for retaining the pupil/student record until the pupil/student reaches the age of 25 years.

There are some instances where we need to keep some of your information until you have reached the age of 21. Where this is necessary your details will be kept securely archived and will only be accessed if and where the need arises. After this period of time has elapsed your details will be securely destroyed through a data-shredding service.

Data sharing

We do not share personal information about you with anyone outside the Trust and its academies without permission from you or your parents/carers, unless the law and our policies permit us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

Third Parties	Reason for Processing	Legal Basis	Type of Information
Warwickshire County Council / Warwickshire Educational Services	Such as safeguarding concerns, exclusions, third party service provision	Public task	Name, age, date of birth, gender, unique pupil number, address
Essex Educational Services and Evolve	To manage, process and record school visit and trip data	Consent	Name
Central and local government	Such as safeguarding concerns, exclusions, third party service provision	Public task	Name, age, date of birth, gender, unique pupil number, address

The Department for Education	Census data	Public task	Name, age, date of birth, gender, unique pupil number
Education and Skills Funding Agency	Funding	Public task	Name, age, date of birth, gender, unique pupil number, FSM
The pupil's family and representatives	Sharing progress and data, pastoral care, securing engagement, trips/visits, complaints, referrals to third party services, seek consent	Consent	Name, age, date of birth, gender, address, medical information
Pupil referral services to support learning and pastoral care	Third party service providers such as Reach/Camhs/Marf	Public task	Name, age, date of birth, gender, unique pupil number, address, medical information
Pupil records services	Third party service providers such as The Learning Records Service	Public task	Name, unique pupil number
Other educational providers such as our curriculum partner schools or services which offer alternative educational provision	Third party service providers such as Warwickshire College, Guilsborough School	Public task	Name, age, date of birth, gender, unique pupil number, medical information
Educators, examining bodies and associated data transfer systems for access arrangements and data transfers to awarding bodies	Third party service providers such as examination boards, testing organisation, awarding bodies, examination regulators and The School Performance Data Unit	Public task	Name, age, date of birth, gender, unique pupil number
Admissions	Third party service providers such as Clerks Associates who manage admission appeals	Public task	Name, age, date of birth, gender, address, medical information, photograph
Destinations data transfers	Third party service providers who monitor post-16 provision and performance	Public task	Name, age, date of birth, gender, qualification outcomes
Provision from contracted service providers	Third party service providers such as Sims, Edulink, GL Assessments, Study Bugs and SISRA	Public task	Name, age, date of birth, gender, home address, photograph; name of parent(s)/carer(s); ethnicity; unique pupil number, medical information, SEN and FSM/PP designations;

			assessment, behavior and attendance history
To enable provision from contracted service providers	Third party service providers such as Kerboodle; Hegarty Maths; MathsWatch; My Maths; Complete Maths; Times Table Rock Stars; GCSEPod; Wix; Viva; Educake; KUDOS, Eclipse Library Service; Prospect for careers advice and guidance	Public task	Name/ username; date of birth; name of school
Website and wireless services,	Third party service providers for such as Google/Drive, Smoothwall and Meraki	Public task	Name/ username Internet history
Financial organisations	Third party service providers such as BioStore (cashless system) and ParentPay	Public task	Biometric fingerprint, name, address, photograph
Our auditors	Third party service providers such as Daines	Public task	Name
Health authorities	Third party service providers such as the NHS	Consent or Vital Interests (if the individual is unable to give their consent)	Name, address, age, date of birth, next of kin, medical information
Public Health England	NHS Test and Trace	Public task	Name, date of birth, year group, parent's contact number, COVID-19 test results
Security organisations	Third party service providers for example for CCTV	Public task	Image
Health and social welfare organisations	Third party service providers to support the pastoral, medical and SEND care and provision	Consent or Vital Interests (if the individual is unable to give their consent)	Name, address, age, date of birth, medical, SEN
Professional advisers and consultants	Third party service providers such as behaviour, attendance and counselling services	Public task	Name, address, age, SEN, FSM
Police forces, courts, tribunals	Third party legal or regulatory organisations	Public task	Name, address, age, medical, SEN, attendance

Colleges and Universities	Post-16 provision, for example university open day visits or interviews	Public task	Name, age, gender, date of birth, qualification outcomes
Tour operators for trips and visits	Third party service providers to enable trips and school visits to occur, for example PGL, Rayburn Tours, World Challenge	Consent	Name, passport, age, date of birth, nationality
Work experience placement organisations	For example where references are required or where a work experience placement is being organised	Public task	Name, age, address, medical, SEN
Emailing and texting services to communicate with parents	Third party service providers such as Click Send and Google Guardian	Public task	Name, phone number, email address

National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school/academy census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools/academies are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, academies, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations, which promote children’s education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education’s webpage on how it collects and shares research data.

You can also contact the Department for Education if you have any questions about the database.

Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to Warwickshire County Council and other third-party youth support services as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Your parents/carers, or you once you’re 16, can contact your academy’s Principal to ask us to only pass your name, address and date of birth.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a ‘**subject access request**’, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request, please contact your academy's Principal.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting your academy's Principal.

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact your academy's Principal.

Appendix 6 - Privacy notice for staff

Under data protection law individuals have a right to be informed about how the Trust and its academies use any personal data that we hold about them. We comply with this right by providing 'privacy notices' to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work within the Trust.

We, Transforming Lives Educational Trust, are the 'data controller' for the purposes of data protection law.

Our data protection officer is provided by Warwickshire Education Services (WES).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work in our Trust. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the Trust, including to:

- Enable you to be paid
- Ensure your tax, national insurance and pension contributions are correct
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Allow financial modelling and planning
- Planning the school's staffing needs
- Provide references where required for your future employment

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds, which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it after 7 years.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

Third Parties	Reason for Processing	Legal Basis	Type of Information
Warwickshire County Council / Warwickshire Educational Services	Such as safeguarding concerns	Public task	Name, DfE number, address, address, gender, criminal record
Essex Educational Services	To manage, process and record school visit and trip data	Consent	Name
Evolve	To manage, process and record school visit and trip data	Consent	Name
Central and local government	Such as safeguarding concerns,	Public task	Name, DfE number, address, address, gender, criminal record

The Department for Education	Regulatory	Public task	Name, DfE number, address, address, gender, criminal record
Ofsted	Regulatory	Public task	Name, DfE number, address, address, gender
Education and Skills Funding Agency	Funding	Public task	Name, DfE number, address, address, gender
Your family and representatives	Emergency contact details	Consent	Name, address, gender, next of kin, medical, telephone number
Disclosure and Baring Service (DBS)	Regulatory	Public task	Name, age, date of birth, DfE number address, gender, criminal record
Teachers' Pension Agency	Pension contributions	Public task	Name, age, date of birth, DfE number address, NI number, salary details
Other educational providers such as our curriculum partner schools	Third party service providers such as Guilsborough School	Consent	Name
Staff Salary Processors	Processing staff salaries	Public task	Name, age, date of birth, DfE number address, NI number, salary details
Third party training organisations such as the National College, our partner schools etc.	To provide professional development training	Consent	Name, professional qualifications
Provision from contracted service providers	Third party service providers for such as Sims	Public task	Name, age, date of birth, DfE number address, NI number, image
To enable provision from contracted service providers	Third party service providers for such as SISRA; Study Bugs; Edulink; Evolve Trips Manager	Public task	Name
Website and wireless services	Third party service providers for such as Google/Drive, Smoothwall, Impero and Senso, Micro Librarian and Meraki	Public task	Name
Financial organisations	Third party service providers such as BioStore (cashless system) and ParentPay	Consent	Name, image, biometric fingerprint

Our auditors	Third party service providers such as Daines	Public task	Name
Health authorities	Third party service providers such as the NHS	Consent or Vital Interests (if the individual is unable to give their consent)	Name, date of birth, medical, address
Public Health England	NHS Test and Trace	Public task	Name, date of birth, contact number, COVID-19 test results
Security organisations	Third party service providers for example for CCTV and Net2 (security doors)	Public task	Name, image, site access events
Event organisation and management	Third party service providers such as Eventbrite	Consent	Name
Health and social welfare organisations	Third party service providers to support medical care and provision	Consent or Vital Interests (if the individual is unable to give their consent)	Name, date of birth, medical, address
Professional advisers and consultants	Third party service providers	Consent	Name
Police forces, courts, tribunals	Third party legal or regulatory organisations	Public task	Name, age, date of birth, DfE number address, NI number, image
Professional bodies	Third party professional organisations, for example in the case of a legal or professional dispute or complaint	Consent	Name
Tour operators for trips and visits	Third party service providers to enable trips and school visits to occur, for example PGL, Rayburn Tours, World Challenge	Consent	Name, address, passport, medical, date of birth

Transferring data internationally

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.

Your rights

How to access personal information we hold about you

Individuals have a right to make a ‘**subject access request**’ to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for

- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact your academy's Principal.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact your academy's Principal.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Appendix 7 - Privacy Notice - Covid-19 Mass Testing.

Transforming Lives Educational Trust – COVID-19 Testing Privacy Statement

Ownership of the Personal Data

To enable Covid-19 testing to be completed at Transforming Lives Educational Trust academies, we need to process personal data for staff and pupils taking part, including sharing of personal data where we have a legal obligation. Transforming Lives Educational Trust is the Data Controller for the data required for processing the tests and undertaking any actions which are needed by its academies to ensure we meet our public health and safeguarding legal obligations.

Personal data relating to tests for pupils is processed under paragraph 7 of the Schedule to the Education (Independent School Standards) Regulations 2014 applicable to academies.

Personal Data relating to staff is processed under the legitimate interest of the Data Controller to ensure we can minimise the spread of Covid-19 in a timely manner, and enable us to continue to deliver education services safely and securely.

The following paragraph is relevant to both pupils and staff taking tests.

If you decline a test, we record your decision under the legitimate interest of academies in order to have a record of your decisions and to reduce unnecessary contact with you regarding testing.

The processing of special category personal data is processed under the provisions Section 9.2(i) of GDPR, where it is in the public interest on Public Health Grounds. This data is processed under the obligations set out in Public Health legislation (Regulations 3(1) and (4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI)) which allows the sharing of data for Covid-19 related purposes and where it is carried out by a health care professional **OR** someone who owes an equivalent duty of confidentiality to that data.

Personal Data involved in the process

We use the following information to help us manage and process the tests:

- Name
- Date of birth (and year group)
- Gender
- Ethnicity
- Home postcode
- Email address
- Mobile number
- Unique barcode assigned to each individual test, which will become the primary reference number for the tests
- Test result
- Parent/guardians contact details (if required)

We will only use information that is collected directly from you specifically for the purpose of the tests, even if you have previously provided us with this information.

How we store your personal information

The information will only be stored securely on local spreadsheets in individual academies whilst it is needed. It will also be entered directly onto DHSC digital services for the NHS Test and Trace purposes. Academies will not have access to the information on the digital service once it has been entered.

Processing of Personal Data Relating to Positive test results

The member of staff, pupil, student or parent (depending on contact details provided) will be informed of the result by the academy and advised how to book a confirmatory test.

We will use this information to enact our own Covid-19 isolation processes, without telling anyone who it is that has received the positive test.

The information will be transferred to DHSC, who will share this with the NHS, GPs. PHE and the Local Government, who will use this information for wider test and trace activities as well as statistical and research purposes.

This information is processed and shared under obligations set out in Public Health legislation under Regulations 3(1) and (4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) which allows the sharing of data for COVID related purposes.

This information will be kept by the academy for up to 14 days and by the NHS for 8 years.

Processing of Personal Data Relating to Negative test results

We will record a negative result and the information will be transferred to DHSC, NHS. PHE and the Local Government, who will use the information for statistical and research purposes.

This information is processed and shared under obligations set out in Public Health legislation under Regulations 3(1) and (4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) which allows the sharing of data for COVID related purposes.

This information will be kept by the academy for up to 14 days and by the NHS for 8 years.

Processing of Personal Data relating to declining a test

We will record that you have declined to participate in a test and this information will not be shared with anyone.

Data Sharing Partners

The personal data associated with test results will be shared with

- DHSC, NHS, PHE – to ensure that they can undertake the necessary Test and Trace activities and to conduct research and compile statistics about Coronavirus.
- Your GP – to maintain your medical records and to offer support and guidance as necessary
- Local Government to undertake local public health duties and to record and analyse local spreads.

When data is transferred to a data sharing partner, Data Controllorship is also transferred. For more information about what they do with your data please see the Test and Trace [Privacy Notice](#). The academy remains the Data Controller for the data it retains about you.

For more information about what happens when your data is transferred to the Department of Education, please read the following, which is taken from their **Privacy Notice - school or college representative contact details for managing delivery of Covid-19 Testing**.

Purpose of processing personal data

To enable Covid-19 testing to be delivered by schools and colleges and supported by the Department for Education (DfE), the DfE needs to process personal data of a designated representative for each school or college. DfE will only use the personal data that is collected from the school or college specifically for the purpose of supporting the delivery of Covid-19 testing in schools and colleges, including the maintenance of an audit record of delivery. A school or college should share this Privacy Notice with their designated representative to ensure the individual is informed of the processing of their personal data by the DfE.

Personal data involved in the process

A school or college will supply to DfE the following information about a designated representative for the above purpose:

- Name of individual
- Work email address
- Work mobile telephone number

linked to the identity (Unique Registration Number) of the school or college

Lawful basis for processing the personal data

When the school or college supplies the personal data to the DfE for the above purpose, the DfE becomes a Data Controller of that data. The DfE processes the personal data as part of its legitimate interest, supporting schools and colleges in the delivery of their public health duty. The DfE will only process the minimum of personal data required to meet the above purpose.

Data sharing partners

The personal data is securely shared by DfE with a third-party data sharing partner (SERCO, a delivery partner of the Department for Health and Social Care) who will only process the personal data on behalf of the DfE for the above purpose.

How we store the personal information

The information will only be stored and shared securely with the DfE's third-party data sharing partner for the above purpose. Only a restricted minimum of individuals within DfE and the third-party data sharing partner will access the personal information for the above purpose.

How long we process your personal data

The minimum of personal information will be retained by DfE and the third-party data sharing partner only for as long as necessary to fulfil the above purpose, following which it will securely destroyed. DfE currently anticipates the information being retained for a minimum of 12 months.

Your Rights

Under data protection law, individuals have rights relating to their personal information, including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you. Please contact us as described below if you wish to make a request.

Further information and how to make a request or complain

Further information about how the DfE processes personal data is published in the DfE's personal information charter. If you have any concerns about our use of your personal information or wish to make a request or complaint to the DfE please use the contact details published in our information charter.

You can also complain to the ICO if you are unhappy with how DfE uses your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow

Cheshire
SK9 5AF

Helpline number: 0303 123 1113