Data Protection Policy

Approved by:	Tyne Coast Academy Trust Board	**Date:** 17 October 2024
Last reviewed:	October 2024	
Next review:	October 2026	

Contents

1. Aims

Tyne Coast Academy Trust ("TCAT", "we", "us", "our") aims to ensure all Personal Data collected about staff, pupils, parents, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with UK Data Protection Law.

This policy applies to all Personal Data, regardless of whether it is in paper or electronic form.

2. Legislation and guidance

This policy meets the requirements of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018").

It also meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the Information Commissioner's Office ("ICO") code of practice for the use of surveillance cameras and Personal Data.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Description:
Accountability	A duty to answer to the success or failure of strategies, decisions, practices and processes
Controller	A person, entity or organisation that determines the purposes and means of processing Personal Data
Criminal Information	Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings
"DPA 2018"	Data Protection Act 2018
Data Protection Impact Assessment ("DPIA")	A DPIA is designed to help an organisation assess the risks associated with data processing activities that could compromise the rights and freedoms of individuals. It can be used to identify and mitigate risk associated with a product, service, business process or other organisational change
Data Protection Law	The UK GDPR, the DPA 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR")
Data Protection Officer ("DPO")	The Data Protection Officer is responsible for overseeing data protection strategy and implementation to ensure compliance with Data Protection Law
Data Subject	Any natural person (individual) whose Personal Data is being processed

“EEA”	European Economic Area – the EU member states plus Norway, Iceland and Liechtenstein
Information Commissioner’s Office (“ICO”)	An independent public body established in the UK responsible for monitoring the application of the UK GDPR, DPA 2018 and PECR
Legitimate Interest Assessment (“LIA”)	Determines if individual’s Personal Data is being used in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing
Personal Data	Any information relating to an identified or identifiable natural person (a “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
Processing	Any operation or set of operations that is performed on Personal Data, such as collection, recording, organising, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, combination, restriction or erasure
Processor	A person, entity or organisation that processes Personal Data on behalf of a Controller
Sensitive Personal Data	Special Category Data and Personal Data relating to criminal convictions and offences
Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, biometric data (where used to identify a Data Subject), data concerning health and data concerning a natural person’s sex life or sexual orientation
“UK”	The United Kingdom – England, Scotland, Wales and Northern Ireland
“UK GDPR”	UK General Data Protection Regulation has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018
“UK IDTA”	UK International Data Transfer Agreement – a mechanism used to legitimise international transfers from the UK to third countries

4. The Controller of Personal Data

Our Trust and academies within the Trust determine the purpose and means of processing Personal Data relating to parents, pupils, staff, trustees, governors, visitors and others, and is therefore a Controller of that Personal Data.

Tyne Coast Academy Trust is registered as a Controller with the Information Commissioner's Office, registration number ZA362655.

5. Roles and responsibilities

This policy applies to all staff employed by our Trust and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action up to and including termination of your contract of employment for serious offences.

5.1 Board of Trustees

The board of trustees has overall responsibility for ensuring our Trust complies with the relevant data protection obligations.

5.2 Data Protection Officer / Data Protection Representative's

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. The DPO is the contact point for the ICO.

The Trust has also appointed a Data Protection Representative ("DPR") in each academy who acts as a first point of contact for individuals whose data the Trust processes and deals with general day-to-day data protection tasks. This person will contact the DPO if necessary. Individual DPR contact details can be found by contacting the relevant academy.

Our DPO is Evalian Limited, available at dpo@evalian.co.uk or 03330 500 111.

5.3 Headteacher/Principal

The Headteacher/Principal of each academy acts as the representative of the Controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any Personal Data in accordance with this policy;
- Informing the Trust/academy of any changes to their Personal Data, such as a change of address; and
- Contacting the DPR or 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 about the lawful basis to use Personal Data in a particular way;
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer Personal Data outside the UK;
    - If there has been a data incident or identified data breach;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals; or
    - If they need help with any contracts or sharing Personal Data with third parties.

6. Data protection principles

The UK GDPR is based on data protection principles with which our Trust must comply.

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; and
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the Trust aims to comply with these principles.

7. Collecting Personal Data

7.1 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:

- The data needs to be processed so that the Trust/academy can **fulfil a contract** with the individual, or the individual has asked the Trust/academy to take specific steps before entering into a contract;
- The data needs to be processed so that the Trust/academy can **comply with a legal obligation;**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life;
- The data needs to be processed so the Trust/academy, as a public authority, can **perform a task in the public interest or exercise its official authority**;
- The data needs to be processed for the **legitimate interests** of the Trust/academy (where the processing is not for any tasks the Trust/academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden; or
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

For processing special categories of Personal Data, we must meet one of the conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**;
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**;
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for the establishment, exercise or defence of **legal claims**;
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation;

- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under UK law;
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law; or
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under UK data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**;
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**; or
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect Personal Data directly from individuals, we will provide them with the relevant information required by UK data protection law, by way of a privacy notice. If we receive Personal Data from a third party, e.g., another school, we will provide a privacy notice to the Data Subject within one month of receipt of the Personal Data.

We will always consider the fairness of our data processing. We will ensure we do not handle Personal Data in ways that individuals would not reasonably expect, or use Personal Data in ways which have unjustified adverse effects on them.

7.2 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, by way of privacy notice.

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 to do their jobs.

We will keep data accurate and, where necessary, up to date.

When staff no longer need the Personal Data they hold, they must ensure it is deleted or anonymised. This will be carried out in accordance with the Trust's Record Management and Retention Policy.

8. Sharing Personal Data

We will not normally share Personal Data with anyone else, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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; or
- 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 UK data protection law;
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any Personal Data we share; and
    - 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.

We may also share Personal Data with emergency services and local authorities to help them respond to an emergency that affects any of our pupils or staff.

Where we transfer Personal Data internationally, we will do so in accordance with UK data protection law.

9. Subject Access Requests and other rights of individuals

9.1 Subject Access Requests ("SARs")

Individuals have a right to submit a SAR to gain access to Personal Data the trust holds about them. This includes:

- Confirmation that their Personal Data is being processed;
- Access to a copy of their Personal Data;
- The purposes of the processing;
- The categories of Personal Data;
- Who the Personal Data has been, or will be, shared with;
- How long the Personal Data will be stored, or if this is not possible, the criteria used to determine this period;
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing;
- The right to lodge a complaint with the ICO;
- The source of the data, if not the individual; and
- Whether any automated decision-making is being applied to their Personal Data and what the significance and consequences of this might be for the individual.

SARs can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of requestor (or requestor's representative);
- Correspondence address;
- Contact number and email address; and

- Details of the information requested.

If staff receive a SAR in any form, they must immediately forward it to the respective DPR.

9.2 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 submit a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR or have given their consent.

In the UK, children aged 12 or under are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils of this age within our Trust may be granted without the express permission of the pupil.

In the UK, children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils of this age within our Trust may not be granted without the express permission of the pupil.

In both cases, this is not set in stone and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 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 (or receipt of the additional information needed to confirm identity, where relevant);
- Will provide the information free of charge; and
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual;
- Would reveal the child being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- Would include another person's Personal Data that we cannot reasonably anonymise and we do not have the other person's consent and it would be unreasonable to proceed without it; or
- It is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO, or they can seek to enforce their right through the courts.

9.4 Other data protection rights
In addition to the right to submit a SAR (see above), individuals 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;
- Object to processing which has been justified based on public interest, official authority or legitimate interests;
- Challenge processing which has been justified based on public interest;
- Challenge decisions based solely on automated decision making or profiling (i.e., making decisions or evaluating certain things about an individual based on their Personal Data with no human involvement);
- Ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances); and
- Make a complaint to the ICO.

If staff receive such a request, they must immediately forward it to the academy DPR, who will consult with the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, can request 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. If the request is for a copy of the educational record, the Trust may charge a fee to cover the supply costs.

This right applies if the pupil concerned is aged 17 or under.

There are certain circumstances in which this access can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils using finger prints to receive school meals 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. The academy will get written consent from the child (if 13 or over) and 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 academy's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for meals in cash, if they wish.

Parents/carers and pupils can 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 Personal Data, irrespective of any consent given by the pupil's parent(s)/carer(s).

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

12. CCTV

We use CCTV in various locations around the academies within our Trust 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.

13. Photographs and videos

As part of our Trust/academy activities, we may take photographs and record images of individuals.

We will obtain written consent from parents/carers (or pupils aged 13 and over) for photographs and videos to be taken of their child (or them) for communication, marketing and promotional materials.

Any photographs and videos taken by parents/carers at Trust/academy events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parties have agreed to this.

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 do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Where the Trust/academy takes photographs and videos, uses may include:

- Within the Trust/academy on notice boards and in Trust/academy magazines, brochures, newsletters, etc;
- Outside of Trust/academy by external agencies such as the academy photographer, newspapers, campaigns; or
- Online on our Trust/academy websites 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.

14. Data protection by design and by default

We will put measures in place to show that we have integrated data protection into all 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 Data Protection Impact Assessments ("DPIAs") where the Trust/academy's processing of Personal Data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
- Integrating data protection into internal documents and any related policies, procedures and privacy notices;
- Regularly training members of staff on data protection, 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;
- Appropriate safeguards put in place if we transfer any Personal Data outside the UK, where different data protection laws will apply; and
- Maintaining records of our processing activities, including:
    - For the benefit of Data Subjects, making available the name and contact details of our academy DPRs and DPO and all information we are required to share about how we use and process their Personal Data (via our privacy notices); and
    - For all Personal Data we hold, maintaining an internal record of the type of data, type of Data Subject, how and why we are using the data, any third-party recipients, any transfers outside the UK (if any) and the subsequent safeguards, retention periods and how we are keeping the data secure.

15. Data security and storage of records

We will protect Personal Data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, accidental or unlawful loss and destruction or damage. 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, 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 academy office;
- Passwords containing at least 8 letters and numbers are used to access Trust/academy computers, laptops and other electronic devices. Staff and pupils are

reminded to change their passwords at regular intervals and not reuse passwords from other sites;
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, pupils, trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust/academy-owned equipment (see our Acceptable use of IT/Information Security Policy); and
- 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).

16. 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 are not required to rectify or update it. For example, we will shred or use the confidential waste process in academies and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data breaches

The Trust will make all reasonable efforts to ensure there are no Personal Data incidents or breaches.

In the event of a data incident or breach, we will follow the procedure set out in the Personal Data Breach Procedure.

If required, we will report any significant data breach to the ICO within 72 hours of becoming aware of it. Such breaches in an academy context may include, but are not limited to:

- A non-anonymised dataset being published on the academy website, which shows the exam results of pupils eligible for the pupil premium;
- Safeguarding information being made available to an unauthorised person; or
- The theft of a Trust/academy laptop containing non-encrypted Personal Data about pupils.

18. Training

All staff and trustees 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's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary, for example if significant changes are made to UK data protection legislation which affect our Trust/academy's practices. Otherwise, this policy will be reviewed annually as per DfE guidance and approved by the Trust Board.

20. Version control

Version Number	Purpose/Change	Author	Approval	Date
1.0	Policy first developed, in line with changes to Data Protection Law	C.Pinkney, Operations Manager	Tyne Coast Academy Trust Board	18/10/2018
2.0	Policy updated to reflect further ICO guidance and clarification	C.Pinkney, Operations Manager	Tyne Coast Academy Trust Board	04/07/2019
3.0	Policy updated to reflect changes due to Brexit and reflect changes to DPO	M Dobrianski HR Manager	Tyne Coast Academy Trust Board	08/07/2021
4.0	Policy annual review and update to reflect changes in UK data protection legislation	Evalian Limited Data Protection Officer	Tyne Coast Academy Trust Board	01/01/2023
5.0	Annual review and update	Evalian Limited Data Protection Officer	Tyne Coast Academy Trust Board	01/10/2023
6.0	Annual review and update	Evalian Limited Data Protection Officer	Tyne Coast Academy Trust Board	17/10/2024