Data Protection Policy

Version Control

Version:	1.2.1
Applies To:	All TPAT employees, Trust Board, Local Monitoring Committees, Contractors, Consultants & Visitors
Date of Review:	TBC
Date of Policy Review Working party approval:	14.05.2025
Review Date:	July 2026
Author:	Christopher Pickles (Director of Operations)
Owner:	Dr Jenny Blunden OBE (Chief Executive Officer)

Document Control

Date	Author	Version	Reason for Change
22/11/2024	CJ Pickles	0.2	Draft to merge existing documentation into one centrally owned document – revision to ownership & additions from DPO
TBC	B Couch	1.2	Approval from Trust Board
29/01/2025	C Pickles	1.2.1	Comments from Trust Board
07/07/2025	C Pickles	1.2.2	Addition of Appendix C

Appendices

A	Breach and Non-Compliance Procedures
B	CCTV Procedures
C	Data Retention Schedule & Disposal Procedures
D	

Contents

Introduction

Truro and Penwith Academy Trust and our academies/schools committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data, and we take that very seriously. This policy, and the Privacy Notices, set out how we look after and use data.

Each school will be responsible for the day-to-day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

The trust central team are responsible for data held centrally about individuals.

Where we use the phrase 'we' that refers to the school/academy/trust and the individual academies/schools.

What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020.

The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and provisions in the Data Protection Act 2018.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is personal data?

Any information that relates to a living person that identifies them. This can be by name, address, or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Privacy Notices that explain how data about specific groups or activities is used and stored are also available. These can be obtained from each school and links on the website to UK GDPR compliance.

What are the key principles of the UK GDPR?

a. Lawfulness, transparency and fairness

Schools must have a legitimate reason to hold the data, we explain this in the Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are times when you cannot withdraw consent as explained in 'Data Subjects' Rights'.

b. Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

c. Limited collection

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

d. Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the individual school.

e. Retention

A retention policy is in place that governs how long records are held for.

f. Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. Please see TPAT Information Security Policy for further detail.

Who is a 'data subject'?
An individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights
Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

These 'Data Subject's Rights' are set out in more detail in the document 'My Rights - A Guide for Data Subjects'.

Subject Access Requests (SAR)
You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This SAR process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if the request is complicated, or the data cannot be accessed.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information by paper or electronic form.

If you wish to complain about the process, please see our Complaints Policy and later information in this DPA policy.

Who is a 'data controller'?
Truro and Penwith Academy Trust is the data controller. They have ultimate responsibility for how the school/academies/and trust central team manage data. They delegate this processing to individuals to act on their behalf, such as the trust central team and the relevant academy/school staff in each setting.

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

As the Data Controller, individuals process data on behalf of the organisation. This can be a member of staff, possibly a committee member or trustee, a consultant or temporary employee.

Who is a 'data processor'?
This is a person or organisation that uses, collects, accesses, or amends the data that the controller has collected or authorised to be collected.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that data controllers require contractual agreements to ensure that this is the case.

Processing data
The trust and the academies/The school must have a reason to process the data about an individual. Our Privacy Notices set out how we use data. The UK GDPR has six conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent/carer
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school

- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data

Processing data is recorded within the school/academy systems.

Data sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education (DfE), health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school/the academy.

Breaches & non-compliance

If there is non-compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non-compliance Procedure and Process needs to be followed (See ANNEX A).

Protecting data and maintaining Data Subjects' Rights is the purpose of this policy and associated procedures.

Consent

As a trust/school, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

This will largely be managed in the individual academies/school.

Consent and renewal

On the trust/school websites we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent, where required, and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For pupils and parents/carers
On joining the school/academy you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection/consent form.

The contact and consent form are reviewed on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available. This is the obligation of each individual to notify the school/academy of changes.

Pupil consent procedure
Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child as required.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of consent
Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

CCTV Procedures

Please also see the CCTV procedures at Annex B. We use CCTV and store images for varying time periods dependent on requirement in accordance with the Annex B. CCTV may be used for:

- detection and prevention of crimes, in the school/academy and on the premises
- student behaviour management, discipline and exclusions
- staff disciplinary and associated processes and appeals
- maintaining a safe environment for the whole school community

Data Protection Officer
We have a named Data Protection Officer (DPO) whose role is to:

- inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- monitor compliance with the UK GDPR and DPA
- provide advice where requested about the data protection impact assessment and monitor its performance
- be the point of contact for Data Subjects if there are concerns about data protection
- cooperate with the supervisory authority and manage the breach procedure
- advise about training and CPD for the UK GDPR

Our DPO is PHP Law, with the named partner, John Walker, contact details are below.

Address: 6 Delamore Park, Cornwood, Ivybridge, PL21 9QP

Email: info@phplaw.co.uk

Physical security
As a trust/an academy/a school we are obliged to have appropriate security measures in place.

In the trust/academy/school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

Each site has a named individual responsible for authorising access to secure areas along with senior leadership team(s)

All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

All sites and locations need to have the suitable security and review measures in place.

Secure disposal
When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

Complaints & the Information Commissioner Office (ICO)
The trust's/academy's/school's complaint policy deals with complaints about data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

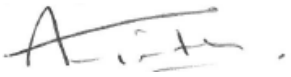
Email: casework@ico.org.uk

Helpline: 0303 123 1113

Website: www.ico.org.uk

Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the DPO every 24 months.

Signed:		Jennifer Blunden	Date:	Chief Executive Officer
Signed:		Anita Firth	Date:	Chair of Trustees
Signed:		Chris Pickles	Date:	Director of Operations

ANNEX A to

Data Protection Policy

BREACH & NON-COMPLIANCE PROCEDURES

Breach management guidance
All staff, governors and trustees must be aware of what to do in the event of a DPA/UK GDPR breach. The 'Data Breach Flowchart' outlines the process.

Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported so that risks to the data subjects are minimized and well managed.

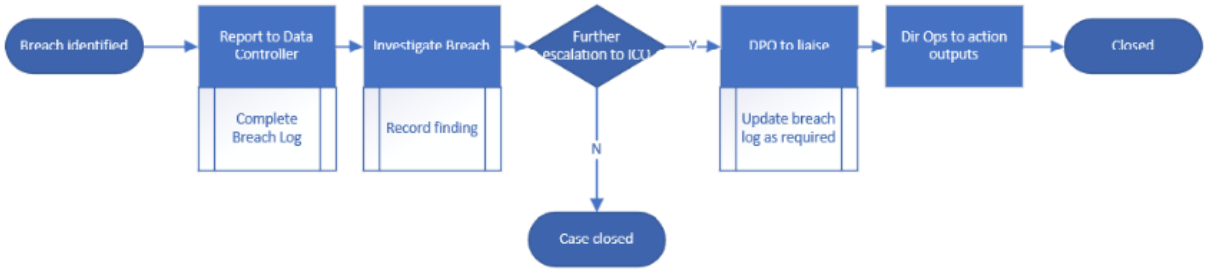
What is a breach?
A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Examples of breaches are:

- information being posted to an incorrect address which results in an unintended recipient reading the information
- loss of mobile or portable device, unencrypted mobile phone, USB memory stick or similar
- sending an email containing personal data to the wrong person
- dropping or leaving documents containing personal data in a public place
- personal data being left unattended at a printer enabling unauthorised persons to read that information
- not securing documents containing personal data (at home or work) when left unattended
- anything that enables an unauthorised individual access to school buildings or computer systems
- discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack which results in unauthorised access to, loss, destruction or damage to personal data

What staff and governors should do?
Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the data controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.



How is the breach managed?
The breach notification form will be completed and the breach registered on the Go-GDPR portal.

Advice will be sought from the Data Protection Officer as required. A plan to effectively manage the breach, who to inform and how to proceed will be put in place.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

Actions and changes to procedures, additional training or other measures may be required to be implemented and reviewed.

The breach report will be within 72 hours of becoming aware of the breach to the Information Commissioner if it is serious.

It may not be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

What happens to the people whose data has been breached?
For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used.

Advice may be taken from the ICO about how to manage communication with data subjects if appropriate.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

What happens next?

The impact of a serious breach will need to be assessed. It may be necessary to change some processes and procedures.

Additional training may be required. IT protocols may need to be reviewed.

The school will work with the Data Protection Officer to ensure that any changes are made to protect and secure information and to learn from any breaches.

ANNEX B to

Data Protection Policy

CCTV Protocols

1. Introduction

Closed Circuit Television (CCTV) Systems are installed in some schools within TPAT. This protocol applies to all schools within TPAT that have CCTV Systems installed.

New CCTV systems will be introduced in consultation with school staff and the Director of Operations (or delegate). Where systems are already in operation, their operation will be reviewed regularly by TPAT IT Operations Manager in consultation with school staff and the Headteacher as required.

2. Purpose

The purpose of this is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of TPAT (this includes all schools and premises within TPAT).

CCTV systems are installed in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

CCTV at TPAT (and its schools/premises) is intended for the purposes of:

- protecting buildings and assets, both during and after school hours;
- promoting the health and safety of staff, students and visitors;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that behaviour policies within schools can be supported.

3. Scope

This protocol relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. Where classes and activities are carried out in rented premises, the IT Operations Manager will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this protocol.

4. General Principles

TPAT as the corporate body for all its schools and premises has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. TPAT owes a duty of care to students, parents, staff and visitors amongst others under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of

life of the school community by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and lawful manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this protocol e.g. CCTV will not be used for monitoring employee performance.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by either TPAT or the individual school, including the provisions set down in equality and other educational and related legislation.

This protocol prohibits monitoring based on the protected characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within a premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

Information obtained in violation of this protocol may not be used in a disciplinary proceeding against an employee of the TPAT or a student attending one of its schools.

All CCTV systems and associated equipment will be required to be compliant with this protocol following its adoption by TPAT. Recognisable images captured by CCTV systems are "personal data" and are therefore subject to the provisions of the Data Protection Act 2018.

5. Justification for use of CCTV

The Data Protection Act 2018 requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that TPAT and the schools within it need to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV to control the perimeter of the school buildings for security purposes has been deemed to be justified by the Board of Trustees. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

In other areas of the school where CCTV has been installed, e.g. hallways, stairwells, TPAT and their schools have demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

6. Location of cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. TPAT and the schools within it have endeavoured to select locations for the installation of CCTCV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas in the schools/premises within TPAT may include the following:

- Protection of buildings and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms
- Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control
- Criminal Investigations (carried out by the police): Robbery, burglary and theft surveillance

7. Covert surveillance

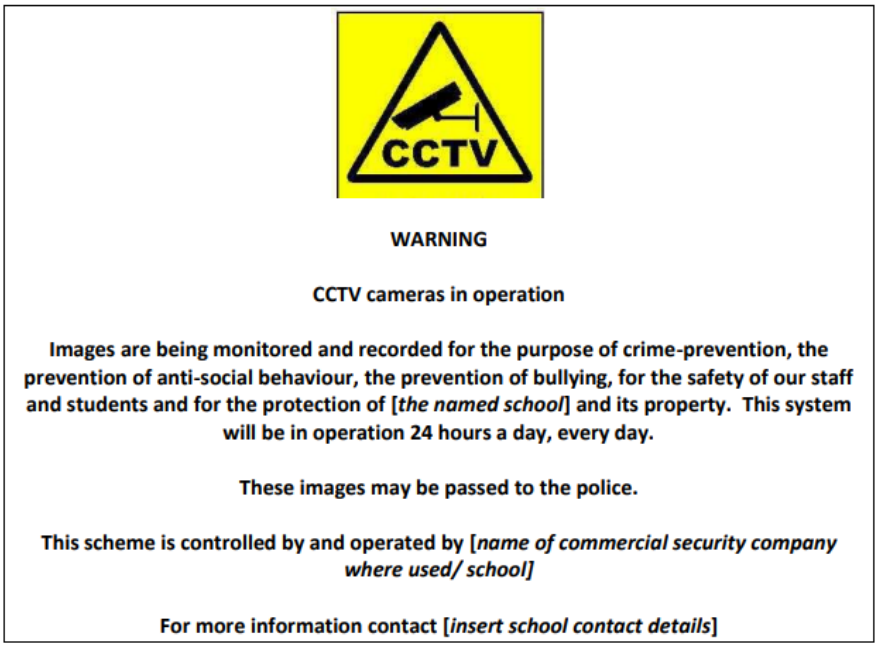
TPAT and the schools within it will not engage in covert surveillance.

Where the police may request to carry out covert surveillance on a premises, such covert surveillance may require the consent of a judge. Accordingly, any such request made by the police will be requested in writing and the school will seek legal advice.

8. Informing / fairness – signage

The school will provide a copy of this CCTV Protocol on request to staff, students, parents and visitors to the school. This protocol describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use and referenced in all Privacy Notices.

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the site. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location. A template for the signage is set out below.



Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, school gates
- reception area
- at or close to each internal camera

9. Storage & Retention

The Data Protection Act 2018 states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the school's Headteacher, who may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Police, the School/Professional Services manager, the relevant Year Head, other members of the teaching staff, representatives of the Department of Education and Skills, representatives of the HSE and/or the parent of a recorded student). When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

10. Access

Tapes/DVDs storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel only.

In relevant circumstances, CCTV footage may be accessed:

- By the police where TPAT, its schools (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the property of TPAT or the schools within it, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the Headteacher in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed; or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to TPAT or one of the schools within it or
- To individuals (or their legal representatives) subject to a court order.
- To the school's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Requests by the police: Information obtained through video monitoring will only be released when authorised by the Headteacher following consultation with TPAT Director of Operations. If the police request CCTV images for a specific investigation, the police may require a warrant and accordingly any such request made by the police should be made in writing and the school must immediately seek legal advice.

Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an SAR in writing to the Headteacher of the relevant school or TPAT (enquiries@tpacademytrust.org) as applicable by location.

A person should provide all the necessary information to assist TPAT and schools within it in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may be considered to be not personal

data and there is no obligation for the image to be handed over by the school. In giving a person a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals must be obscured before the data is released.

11. Responsibilities

TPAT Operations Manager will:

- Ensure that the use of CCTV systems is implemented in accordance with this protocol
- Support headteachers in allowing them to oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within their school
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this protocol
- Ensure that the CCTV monitoring within their school is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system
- Ensure that monitoring recorded tapes are not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. *NOTE: [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by the Police].*
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the CEO.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas

- Ensure that where the Police request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Director of Operations

SECURITY COMPANIES

Where the school's CCTV system is controlled by a security company locally contracted by the school. The following applies:

The school has **a written contract with the security company in place** which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply. The written contract also states that the security company will give the school all reasonable assistance to deal with any subject access request made under the Data Protection Act 2018 which may be received by the school within the statutory time-frame (which is 30 days except for complex cases which are unlikely to apply in case of images captured on a security camera).

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors." As data processors, they operate under the instruction of data controllers (their clients such as TPAT). The Data Protection Act 2018 place a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company has been made aware of their obligations relating to the security of data.

12. Implementation & Review

The protocol will be reviewed and evaluated alongside the wider Data Protection Policy. Ongoing review and evaluation will take cognisance of changing information or guidelines (e.g. from the ICO, the police, Department of Education and Skills, Audit units (internal and external to the school/) national management bodies, legislation and feedback from parents/guardians, students, staff and others). The date from which the policy will apply is the date of adoption by the Board of Trustees. Implementation of the policy will be monitored by the Head teacher of the school.

ANNEX C to

Data Protection Policy

Data Retention Schedule & Disposal Procedures

1. Introduction

The following sets out how long Truro and Penwith Academy Trust (TPAT) will retain information for and the procedures for correct disposal of information.

2. Data Retention Periods

All data held by TPAT is as per guidance set by the Department of Education[1] as follows:

Document Type	Retention Period	Action at End of retention period	Further Information
Primary school pupil records	Until the pupil leaves the school.	Transfer to secondary school or other primary school when the pupil leaves.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the pupil record. There is guidance on how to transfer information to another school.
Secondary school pupil records	Until the pupil's 25th birthday.	Dispose of records securely. If the pupil leaves to go to another school, transfer the records to that school.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the education record. Retain as detailed in section 2 of the Limitation Act 1980. There is guidance on what to do if the academy closes before the end of the retention period.
Special educational needs and disabilities (SEND), including reviews and education, health, and care (EHC) plans	6 years from the cessation of the EHC plan.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980. Regulation 17 of The Special Educational Needs and Disability Regulations 2014.
Child protection files	Until the child's 25th birthday. If the file relates to child sexual abuse, retain	Dispose of records securely. Child protection files should be passed on to any new school a child attends. This should be	Should be stored either as a separate file or in a sealed envelope in the pupil file. Keeping children safe in education, sections 122 and 123. The Report of the Independent

[1] Department of Education (2025) *Data Protection In Schools.* Available at: https://www.gov.uk/guidance/data-protection-in-schools/record-keeping-and-management (Accessed: 03 July 2025).

	until the child's 75th birthday.	transferred as separately from the main pupil file.	Inquiry into Child Sexual Abuse (IICSA) recommendation on access to records.
Allegations of child protection against a member of staff, including unfounded allegations	Until the staff member's normal retirement age, or 10 years from the date of the allegation, whichever is later.	Dispose of records securely.	Keeping children safe in education. Working together to safeguard children.
Contracts	6 years from the last payment on the contract.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Debtor's records	6 years from end of the financial year.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
VAT records	6 years from finance year end.	Dispose of records securely.	May include invoices, budgets, bank statements and annual accounts. Record keeping (VAT Notice 700/21).
Admissions	6 years from the admission date.	Dispose of records securely.	Regulation 7 of the School Attendance (Pupil Registration) (England) Regulations 2024.
Attendance registers	6 years from the date of entry.	Dispose of records securely.	Regulation 7 of the School Attendance (Pupil Registration) (England) Regulations 2024.
Annual governors' report	10 years.	Dispose of records securely.	The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002. Retain as detailed in section 2 of the Limitation Act 1980.
Curricular record	At least 1 year.	Dispose of records securely.	The Education (School Records) Regulations 1989. Regulation 3 of the Education (Pupil Information) (England) Regulations 2005.
Directors – disqualification	15 years from the date of disqualification.	Dispose of records securely.	The Education (Company Directors Disqualification Act 1986: Amendments to Disqualification Provisions) (England) Regulations 2004

Records of educational visits	10 years from the date of the visit. If there was an incident on the visit, retain the permission slips for all pupils and the incident report in the pupil record.	Dispose of records securely.	Health and safety on educational visits. Retain as detailed in section 2 of the Limitation Act 1980.
School vehicles	6 years from the disposal of the vehicle.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Statutory registers and compliance	Retention periods vary, for example: Memorandums of understanding should be retained for the life of the academy plus 6 years. Annual reports should be retained for 10 years from the date of the report. Board meeting records should be retained for 10 years from the date of the meeting.	Dispose of records securely.	May include annual reports and governance records. Companies Act 2006 contains information on which statutory registers to keep. Compliance guidance in the maintained schools governance guide. Compliance guidance in the academy trust governance guide. Academy trust handbook.
Accessibility plans	Life of plan plus 6 years.	Dispose of records securely.	Retain as detailed in section 2 of the Limitation Act 1980.
Accident records	3 years from the date of the accident.	Dispose of records securely.	Accidents involving pupils should be retained in the pupil record. Regulation 25 of the Social Security (Claims and Payments) Regulations 1979.
Monitoring exposure to substances hazardous to health, including asbestos	5 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002.
Health surveillance records	40 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.
Other health records of staff	While the worker is employed in your school.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. HSE guidance on Health surveillance - Record keeping.

Fire assessments	Life of the risk assessment plus 6 years.	Dispose of records securely.	Fire Service Order 2005. Retain as detailed in section 2 of the Limitation Act 1980.
Maintenance records	6 years from finance year end.	Dispose of records securely.	Record keeping (VAT Notice 700/21).
Title deeds	12 years from end of deed.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Copies of DBS certificates	6 months from date of recruitment.	Dispose of records securely.	Keeping children safe in education.
Maternity pay records	3 years after the end of the tax year in which the maternity pay period ends.	Dispose of records securely.	The Statutory Maternity Pay (General) Regulations 1986.
Pay records	3 years from the end of the tax year they relate to.	Dispose of records securely.	PAYE and payroll for employers: Keeping records.
Personnel files	6 years from termination of employment.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Retirement benefits	A minimum of 6 years from the end of the year in which the accounts were signed.	Dispose of records securely.	Regulation 15 of the Retirement Benefits Schemes (Information Powers) Regulations 1995.

3. Data Disposal Procedure

When records have reached the end of their retention period, data must be disposed of securely and confidentially. The ICO has guidance on practical methods for destroying records that are no longer needed.

All records containing personal information or sensitive policy information must be made either unreadable or so you cannot reconstruct it.

Do not dispose of records with the regular waste or in a skip.

All TPAT employees will:

- shred paper records using a cross-cutting shredder, or get an external company to shred them
- destroy storage media and hard disks to particles no larger than 6mm
- dismantle and shred audio and video tapes

If you use an external company to destroy records, it must:

- shred all records on-site in the presence of an employee
- be able to prove that the records have been destroyed and provide a certificate of destruction
- have trained its staff in the handling of confidential documents

The Freedom of Information Act 2000 requires you to maintain a list of records that have been destroyed and who authorised their destruction. You must have approval from a senior leader for the record to be destroyed.

You must document the destruction. Record a brief description of the data, the number of files and who authorised the destruction. Shred the records as soon as you've documented them as having been destroyed. A suggested template is below which can be either used by a supplier or adapted internally:

Please sign the following declaration and return this letter to TPAT Data Protection, keeping a copy for your own records. Should you have any queries, please contact TPAT Data Protection *dataprotection@tpacademytrust.org*

Return electronically. Electronic signatures or otherwise positive confirmation are accepted:

Date: _____

We hereby confirm that all xxxx data, including non-proprietary data generated through the provision of educational services has been suitably, appropriately, and irreversibly destroyed in its entirety and rendered permanently inaccessible and void.

Data backup, including disaster recovery systems, will automatically conduct appropriate data destruction as part of an automated data life cycle on or before the _____ (Strike as applicable)

Anonymised and/or non-Personal Data has been retained for statistical analytical purposes only. We warrant compliance with all applicable data protection and privacy legislation in this regard. (Strike as applicable)

Contract/project reference: _____

For and on behalf of organisation: _____

Name: _____

Position: _____

Date: _____

Description of record(s)	Date range(s) of records	Approximate quantity	Format (for example shared drive folder, SharePoint list, paper, hard drive)	Business unit or function	Name of authoriser	Method and place of destruction	Date of destruction and staff member who carried out the destruction