THE PRIORY
LEARNING TRUST

CCTV Policy

Approved and Authorised for use by the Trust Board 18th July 2023

History of Policy Changes

Date	Version	Change	Origin of Change	Changed by
May 2019	1	Creation of TPLT Policy	Annual Review	Simon Merrick
May 2020	1.1	Updated	Terminology , consistency and InfoSec Alignment	Simon Merrick
May 2021	1.2	Updated	Users who realistically access the CCTV system, Director of IT now Head of IT	Simon Merrick
June 2022	1.3	Updated		Simon Merrick

This policy applies to all schools in The Priory Learning Trust (TPLT)

Date policy adopted	September 2022
Review cycle	Annual
Review date	June 2023

Contents

1. Policy statement

1.1 The Priory Learning Trust (TPLT) uses closed circuit television (CCTV) and the images produced to prevent or detect crime, to monitor its buildings and grounds in order to provide a safe and secure environment for its students, staff and visitors, to support the effective management of student behaviour, to facilitate the identification of and/or to corroborate the occurrence of, any activity or event which might warrant disciplinary action being taken against students or staff, and to prevent loss or damage to its property.

1.2 The system comprises a number of fixed cameras, images from which are transmitted to and stored on Network Video Recorders (NVR) which are located in secure locations. Access to the system is via username and password protection, which is determined by the Academy Network Manager.

1.3 Each Academies CCTV Privacy Impact Assessment policy has a plan showing the location of all of the cameras. The systems do not record sound. The system operates 24 hours a day, 365 days a year.

1.4 The CCTV system is owned and operated by TPLT, the deployment of which is determined by the Chief Operations Officer under the supervision of the Trust's Data Controller. The day to day operation of the system is managed by the Academy Network Manager.

1.5 TPLT's CCTV Scheme at each academy is registered with the Information Commissioner under the terms of the General Data Protection Regulation (UK GDPR). The use of CCTV, and the associated images are covered by the UK GDPR. This policy outlines TPLT's use of CCTV and how it complies with the UK GDPR law.

1.6 The operation of the system and this policy will be reviewed annually and will include, as appropriate, consultation with interested parties.

2. Statement of Intent

2.1 TPLT complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure that CCTV is used responsibly and safeguards both trust and confidence in its continued use.

2.2 CCTV warning signs are clearly and prominently placed at the main reception areas of the academy sites.

2.3 The original planning, design and installation of CCTV equipment endeavoured to ensure that the system would deliver maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

2.4 Materials or knowledge secured by way of CCTV will not be used for any commercial purpose. Recorded materials will only be released to the media with the written authority of the Police or a Court of Law, typically for use in the investigation of a specific crime.

3. Access

3.1 Access to the system will be strictly limited to selected members of the IT teams managing the system, who will receive appropriate instruction on their legal and organisational responsibilities and the terms of the ICO CCTV Code of Practice.

3.2 Cameras may not be relocated or re-positioned without the agreement of each Academy Operations Manager and Trust Head of IT.

4. Covert Monitoring

4.1 It is not TPLT's policy to conduct 'covert monitoring' unless there are 'exceptional reasons' for doing so.

4.2 TPLT may, in exceptional circumstances, determine a sound reason to set up covert monitoring. For example: i) Where there is good cause to suspect criminal activity or malpractice is taking place, or where there are grounds to suspect serious misconduct; ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording. In these circumstances' authorisation must be obtained from the Trustees and the Academies 'Data Controller' advised before any commencement of such covert monitoring.

4.3 Covert monitoring must cease following completion of an investigation.

4.4 Covert monitoring will not be undertaken for the purposes of assessing an employee's performance at work.

5. Storage and Retention of CCTV images

5.1 Recorded data will be retained on the NVR for 31 days after which it will be automatically overwritten.

5.2 The Academy Network Manager will, subject to the completion of a CCTV request form (signed by a senior member of staff), produce a DVD (or similar media extract such as through permission-based Google Drive sharing) of an incident or occurrence. The Academy Network Manager must maintain a log of all such requests including, the date of the request, the date and time of and a brief description of the images requested, the number of copies produced (or method of sharing), and to whom the media was/were given. It is required that such media is kept in secure storage, whether on or off site, as a condition of their approval. This footage will be deleted and/or destroyed when no longer required.

6. Subject Access Requests (SAR)

6.1 The UK GDPR provides that "Data Subjects" (individuals to whom "personal data" relates) with a right to request copies of data held by others about themselves which may include CCTV images.

6.2 If the Data Subject is not the focus of the footage i.e., they have not been singled out or had their movements tracked then the images are not classified as “personal data” and the Data Subject/individual is not entitled to the image under the UK GDPR.

6.3 All requests should be made in writing to the local academy Data Controller. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

6.4 The Trust will respond to requests within 30 calendar days of receiving the written request and any fee. This is as per the ICO CCTV Code of Practice.

6.5 The Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

7. Access to and Disclosure of Images to Third Parties

7.1 There will be no disclosure of recorded data to third parties other than as required by law and to authorised personnel such as service providers to the Trust where these would reasonably need access to the data (e.g. investigations).

7.2 Requests for images / data should be made in writing to the relevant local academy Data Controller.

7.3 Images captured via the system may be used for the purposes of the Trust’s student behaviour and staff discipline and grievance procedures subject to the terms of this policy and to the confidentiality requirements of those procedures.

8. Complaints

8.1 Complaints and enquiries about the operation of CCTV within TPLT should be directed to the relevant local academy Data Controller.

9. Policy Review

9.1 The working of this policy will be reviewed by the Trustees annually. As well as examining the specific review data, the policy statement will be checked for continuing relevance against any changed statutory requirements.