



The Tiffin Girls' School

CCTV POLICY

ADOPTED November 2024

Introduction

1. A Closed-Circuit Television (CCTV) System is in place at The Tiffin Girls' School. This system, known as the 'CCTV System', comprises a number of cameras installed at strategic locations. All of the cameras are fully operational and are recording images only.
2. For the purpose of this policy, the 'Owner' of the system is The Tiffin Girls' School.
3. For the purposes of the Data Protection Act 2018 ('DPA'), the 'Data Controller' is The Tiffin Girls' School.
4. This policy will be subject to review periodically, but at least biannually, to include consultation with interested parties.
5. Throughout this policy it is intended, as far as possible, to balance the objectives of the CCTV System with the need to safeguard the individual's rights. Every effort has been made throughout this policy to indicate that a formal structure has been put in place for the use and processing of the CCTV system and its recordings.

Purpose and Scope of this policy and the use of CCTV in the school

6. The purpose of this policy is to set out how the CCTV system will be used, who is responsible for monitoring the system and how The Tiffin Girls' School will comply with its obligations under the DPA and General Data Protection Regulations (GDPR) 2018.
7. CCTV is used in school to protect the buildings and its assets, to protect the health and safety of students, staff and visitors and to help detect, prevent and reduce incidence of criminal activity.
8. The lawful basis for using CCTV footage is to allow the school to perform the public task of offering education and safeguarding of pupils whilst keeping the premises safe.
9. This policy should be read in conjunction with the Data Protection Policy, the Safeguarding and the Health and Safety Policies.

Roles and Responsibilities

10. The Headteacher is the overall manager of the CCTV System and responsible for ensuring the objectives and principles set out in this policy are upheld.
11. Key Personnel have day-to-day responsibility for the monitoring, operation and evaluation of the CCTV System and the implementation of this policy. The Operations Director is responsible for maintaining full information as to the incidents dealt with in the management of the CCTV System.

- 12.** The following members of staff have authorisation to access the CCTV footage:
- Headteacher
 - Senior Deputy Head / Data Protection Officer (DPO)
 - Operations Director
 - CCTV Manager – IT contractor
 - Caretakers
 - Leisure Assistants, whilst on site and duty. Live access only.
 - Anyone else with the express permission of the Headteacher, DPO or Operations Director
- 13.** CCTV software is installed on individual computers and is password-protected, and only accessible to those people confirmed in paragraph 12. Offices of those concerned are kept locked when not attended.

Principles

- 14.** The CCTV System is registered with the Information Commissioners Officer and the relevant signs are displayed around site to notify people of the use of CCTV.
- 15.** The CCTV System is operated in accordance with the DPA 2018 and the Information Commissioner’s Code of Practice at all times.
- 16.** The CCTV System is operated in accordance with all the requirements and the principles of the Human Rights Act 1998.
- 17.** The CCTV System is operated fairly, within the law, specifically GDPR, and only for the purposes for which it was established and those identified within this policy.
- 18.** The public interest in the operation of the system is recognised by ensuring the security and integrity of operational procedures.

Cameras and Area Coverage

- 19.** The areas covered by CCTV, to which this policy refers, are the buildings and grounds of The Tiffin Girls’ School.
- 20.** None of the cameras forming part of the system are installed inside the property, except for main door foyer.
- 21.** The school will make every effort to position cameras so that their coverage is restricted to The Tiffin Girls’ School premises, which also includes outdoor areas.
- 22.** CCTV will not be used indoors, and cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilet cubicles.
- 23.** Covert Monitoring may be set up in exceptional circumstances. For example:
- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.
 - Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

24. In these circumstances authorisation must be obtained from the Headteacher. Covert monitoring must cease following completion of an investigation.
25. Unless required for evidential purposes or the investigation of crime or otherwise required by law, covertly recorded images will be retained for no longer than 15 days from the date of recording.

Monitoring Equipment

26. The CCTV System records the images from all cameras in real time.
27. Access to the cameras, operating controls, recording and reviewing equipment is strictly limited to authorised personnel only.
28. Any authorised person operating the cameras always acts with utmost integrity.
29. Any replay of pre-recorded data is only undertaken in restricted areas.
30. Unauthorised persons do not have access to any part of the CCTV System without the authorisation of the Operations Director.
31. All CCTV operators receive training relevant to their role. Further training is provided as necessary.

Privacy and Data Protection

32. All personal data obtained by virtue of the system, is processed fairly and lawfully and, in particular, will only be processed in the exercise of achieving the stated objectives of the CCTV System. In processing personal data, there is total respect for everyone's right to privacy.
33. The storage and security of the data will be strictly in accordance with the requirements of the DPA, the Information Commissioner's Code of Practice and the School's Data Protection Policy.
34. All data is processed in accordance with the principles of the DPA, which are set out in the Data Protection Policy.
35. Security measures are in place to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of information.
36. Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the school to ensure that the proposed installation is compliant with legislation and ICO guidance.

Maintenance of the CCTV System

37. Provision is made for regular/periodical service checks of the CCTV equipment, which includes cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.
38. Key Personnel as defined in paragraph 12 have full responsibility for all technical hardware aspects of the CCTV system. Should a fault develop all cameras, servers, switches and computers have maintenance and warranty agreements in place.

39. Key Personnel will maintain appropriate records in respect of the functioning and maintenance of the cameras.
40. Key personnel will carry out monthly PPM checks on the CCTV software and equipment to ensure the system is functioning to required standards and no quality loss is evident.

Handling of recorded material

41. For the purposes of this policy 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of the CCTV system, but specifically includes images recorded digitally, on hard drive and by way of DVD copying, including digital video prints.
42. Subject to the equipment functioning correctly, images from the cameras are recorded throughout every 24-hour period.
43. Recorded footage is retained for a period of 15 days, unless there is a specific purpose for which it is retained for a longer period of time.
44. Every digital recording obtained by using the CCTV System has the potential of containing recorded material, which may have to be admitted in evidence at some point during its life span. Irrespective of the format (e.g. DVD, paper copy, etc.), images obtained from the CCTV system are treated strictly in accordance with this policy from the moment they are received until their final destruction.
45. Access to, and the use of, recorded material is strictly for the purposes defined in this policy.
46. Recorded material is not copied, sold, or used for commercial purposes or the provision of entertainment.
47. In complying with the DPA and GDPR 2018, it is intended, as far as reasonably practicable, to safeguard individual rights to privacy and ensure that the recorded material shall be processed lawfully and access restricted at all times.
48. The recorded material should not be viewed by anyone other than authorised personnel unless this is permitted by the Headteacher in consultation with the DPO or the Operations Director as stated in paragraph 12.
49. It may be beneficial to make use of 'real' digital recordings for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention, and detection of crime. Any material recorded by virtue of the CCTV system is only used for such training and education purposes.
50. A digital image is a copy of an image or images, which already exists on a hard drive or DVD. Digital images are not taken as a matter of routine. The Headteacher and Data Protection Officer, must authorise any requests to make digital images from the CCTV System. There must be a good reason for the request. If a digital image is made, the purpose of the request is recorded. The record will include brief details of the nature of the incident together with the location, time and date.
51. If a digital image is required in connection with a criminal investigation, it is treated as an exhibit and dealt with in accordance with the rules of evidence in respect of continuity, disclosure and any further requirements as set out by the police or prosecuting authority.

Copyright

52. Copyright and ownership of all material recorded by virtue of the CCTV System remains with the Data Controller.

Requests for access to records

53. The DPA 2018 provides that Data Subjects (individuals to whom 'personal data' relate) have a right to request data held about themselves, including those obtained by CCTV.
54. If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Operations Director and/ or IT managed service provider will take appropriate measures to ensure that the footage is restricted in this way.
55. The Tiffin Girls' School will not provide a copy of CCTV footage to anyone else other than a) the police or other law enforcement agencies and/or b) insurers or their legal representatives who make a request as part of an investigation into an ongoing claim.
56. A record will be kept of when the access was requested, the process undertaken to honour the request and the date, if relevant, of when the images were accessed.

Public Information

57. The school will only disclose recorded CCTV images to third parties or public where it is permitted to do so in accordance with the Data Protection Legislation.
58. Warning signs are in place at the school in areas covered by the CCTV system. The signs indicate the presence of CCTV monitoring.
59. If a request is received from a law enforcement agency for disclosure of CCTV images then the premises and/or IT managed service provider must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.
60. The information above must be recorded in relation to any disclosure.

Review

61. This policy will be reviewed when needed or at least every two years.

Complaints

62. Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

Breaches of this policy

- 63.** Any breach of this policy is initially investigated by The Headteacher, for the appropriate action to be taken.

- 64.** All authorised operators and staff with access to images are aware of the procedures that need to be followed when accessing the recorded images. All members of staff who have access will undergo training to ensure proper handling of the system and footage. Authorised staff are aware of the restrictions in relation to access to and disclosure of recorded images. CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors. Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action should investigations by the Operations Director and DPO conclude so.