

CCTV Policy



ADOPTED	September 2018
REVIEWED	September 2021
NEXT REVIEW	September 2022

Contents

1. Policy Statement	3
2. Purpose of CCTV	3
3. Description of System	3
4. Siting of Cameras	3
5. Privacy Impact Assessment	3
6. Management and Access	4
7. Storage and Retention of Images	4
8. Disclosure of Images to Data Subjects	5
9. Disclosure of Images to Third Parties	5
10. Review of Policy and CCTV System	6
11. Misuse of CCTV Systems	6
12. Complaints Relating to this Policy	6
13. History of Changes	6
14. Appendices	8
<i>Appendix 1 Location and Purpose of CCTV Cameras</i>	<i>9</i>
<i>Appendix 2 Authorised Users</i>	<i>11</i>
<i>Appendix 3 CCTV User Rules</i>	<i>12</i>

1. Policy Statement

The Spires College uses Closed Circuit Television (CCTV) within the College premises. The purpose of this policy is to set out the position of the College with regard to the management, operation and use of the CCTV at the College.

This policy applies to all members of our workforce, visitors to The Spires College and all other persons whose images may be captured by the CCTV system.

This policy takes account of all applicable legislation and guidance, including:

- ▲ The General Data Protection Regulation (GDPR);
- ▲ Data Protection Act 2018 (together the Data Protection Legislation);
- ▲ CCTV Code of Practice produced by the Information Commissioner;
- ▲ Human Rights Act 1998.

2. Purpose of CCTV

The Spires College uses CCTV for the following purposes:

- ▲ To provide a safe and secure environment for students, staff and visitors;
- ▲ To prevent the loss of or damage to The Spires College buildings and/or assets;
- ▲ To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

3. Description of System

The Spires College uses fixed and moveable cameras on its main site and in the football stand undercroft. Cameras are not equipped for sound recording.

4. Siting of Cameras

All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, students and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The College will make all reasonable efforts to ensure that areas outside of the College premises are not recorded.

Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

Cameras may be located in classrooms and where this is the case employees and students will all be aware. Access to the footage from such cameras will only be used to fulfil the purposes described in Section 2 of this policy.

The locations and purposes of CCTV cameras at The Spires College are described in Appendix 1.

5. Privacy Impact Assessment

Prior to the installation of any new CCTV camera, or system, a privacy impact assessment will be conducted by the College to ensure that the proposed installation is compliant with legislation and ICO guidance.

Unless there is a material change in risk, existing CCTV cameras and systems will be reviewed and a privacy impact assessment carried out at least every three years.

The Spires College will take a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6. Management and Access

The CCTV system is provided and maintained by the College's PFI Provider in the College and the Football Stand which is an annexe under the direct control of the College. The College and the PFI Provider have agreed to use the same CCTV contractor to maintain this as a single integrated system.

The College has a Responsible Person with control of CCTV operations. The Responsible Person is Tony Jordan, College Business Manager.

Any allegations against staff will be referred immediately to the Principal and only they will determine who needs to view the footage.

On a day to day basis, the CCTV system will be operated by staff with delegated authority. Authorised persons are inducted in the use of the system and Data Protection requirements. The system can only be operated by authorised persons and the system is password protected. The password can only be issued by the Responsible Person. A list of authorised persons is provided in Appendix 2. Authorised persons are inducted in the use of the system as described in Appendix 3.

The viewing of live CCTV images will be restricted to the authorised persons who will ensure that, in doing so, the purposes described in Section 2 of this policy are satisfied.

The viewing of recorded CCTV images will be restricted to the authorised persons who will ensure that, in doing so, the purposes described in Section 2 of this policy are satisfied.

No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

The CCTV system is checked daily to ensure that it is operating effectively.

7. Storage and Retention of Images

Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

Recorded images are stored for a period of no more than 28 days unless there is a specific purpose for which they are retained for a longer period.

The Spires College will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of recorded images. The measures in place include:

- ▲ CCTV recording systems being located in restricted access areas;
- ▲ The CCTV system being password protected;
- ▲ Restriction of the repositioning of cameras to the Responsible Person only;
- ▲ Restriction of the ability to make copies to the Responsible Person.

Images can only be copied and retained with the authority of the Responsible Person who will determine the method of recording, whether any masking is necessary to protect the privacy of other parties, and issue instructions to any third party concerning the correct use of images.

8. Disclosure of Images to Data Subjects

Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has the right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to Data Protection Legislation. Such a request will be considered in the context of the College's Data Protection Policy and Privacy Notices.

When such a request is made, the Responsible Person will review the CCTV footage, in respect of the relevant time periods where appropriate, in accordance with the request.

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 the footage which contains only the images of individual making the request. The Responsible Person must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals then the Responsible Person must consider whether:

- ▲ The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
- ▲ The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained, or;
- ▲ If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the person making the request.

A record must be kept, and held securely, of all disclosures, which sets out:

- ▲ When the request was made;
- ▲ The process followed by the Responsible Person in determining whether the images contained third parties;
- ▲ The considerations as to whether to allow access to those images;
- ▲ The individuals that were permitted to view the images and when; and
- ▲ Whether a copy of the images was provided and, if so, to whom, when and in what format.

9. Disclosure of Images to Third Parties

The Spires College will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with Data Protection Legislation.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

If a request is received from a law enforcement agency for disclosure of CCTV images, the Responsible Person must follow the same procedures 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 enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

The information above must be recorded in relation to any disclosure.

If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires.

If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10. Review of Policy and CCTV System

This Policy, the CCTV system and the privacy impact assessment relating to it will be reviewed, at least, every three years.

11. Misuse of CCTV Systems

The misuse of CCTV systems could constitute a criminal offence.

Any member of staff who breaches this policy may be subject to disciplinary action.

12. Complaints Relating to this Policy

We take any complaints about our collection and use of personal information very seriously. If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance.

To make a complaint, please contact our Data Protection Officer, Jane Richardson, using dpo@thespirescollege.com

Alternatively, you can contact the Information Commissioner's Office:

- ▲ online at <https://ico.org.uk/concerns>
- ▲ by telephone on 0303 123 1113
- ▲ by writing to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

13. History of Changes

Date	Change	Where?
September 2021	Change to details of management of CCTV system	Section 6
September 2021	Removal of references to CCTV access log	Section 7 Appendix 3
September 2021	Locations of CCTV cameras updated	Appendix 1
September 2021	Authorised personnel updated	Appendix 2

CCTV Responsible Person Contact Details

Name	Tony Jordan
Email Address	tjordan@thespirescollege.com
Telephone Number	01803 400660
Postal Address	The Spires College, Westlands Lane, Torquay, TQ1 3PE

Data Protection Officer Contact Details

Name	Jane Richardson
Email Address	dpo@thespirescollege.com
Telephone Number	01803 400660
Postal Address	The Spires College, Westlands Lane, Torquay, TQ1 3PE

14. Appendices

Appendix 1 Location and Purpose of CCTV Cameras

Location	Purpose	Notes
Entrances and exits to building, perimeter fences	Managing visitor access Site security Trespass prevention Protection of assets	Includes rear access lane and bin store
Car Parking areas	Site security Protection of assets	Westlands Lane and Access Lane parking areas
Playground areas	Behaviour management Investigation of accidents and near misses Protection of assets	
Circulation spaces (corridors, stairwells)	Behaviour management Investigation of accidents and near misses Protection of assets	
Communal areas in student toilet blocks	Protection of assets Behaviour management Safeguarding of students and staff	0500 block toilets 1300 block toilets 1400/1600 block toilets MFL lobby toilets 2300 block toilets
Canteen and Milk Bar	Behaviour management Investigation of accidents and near misses Revenue protection Protection of assets	
Canteen cash top up kiosks Canteen till points	Revenue protection Protection of assets	GF corridor and Canteen
ICT classrooms	Protection of assets Investigation of accidents and near misses Behaviour management	Teaching rooms and "drop in" rooms
Music classrooms	Protection of assets Investigation of accidents and near misses Behaviour management	
Music practice rooms	Protection of assets Behaviour management Safeguarding of students and staff Investigation of accidents and near misses	
Main Hall	Protection of assets Management of "public" events Investigation of accidents and near misses	

Location	Purpose	Notes
	Behaviour management	
Sports Hall and Dance Studio	Protection of assets Management of "public" events Investigation of accidents and near misses Behaviour management	
SEND base	Protection of assets Behaviour management Safeguarding of students and staff Management of "public" events Investigation of accidents and near misses	Monitor screen in SENDCO office for base management.
Library	Behaviour management Investigation of accidents and near misses Protection of assets	
Staff Room	Protection of assets	
Visitor Interview Room	Safeguarding of students and staff	
Uniform Shop	Revenue protection Protection of assets Safeguarding of students and staff	
Staff Training Room (0613)	Management of "public" events Protection of assets	
Fitness Suite	Protection of assets Management of "public" events Investigation of accidents and near misses Behaviour management Trespass prevention	In TUFC spectator stand
6 th Form centre	Protection of assets Investigation of accidents and near misses Behaviour management	ICT workrooms and common room Monitor screen in Head of 6 th Form and Deputy Head of 6 th form for centre management

Appendix 2 Authorised Users

Responsible Person

- ▲ Tony Jordan, College Business Manager

Senior Leadership Team

- ▲ Alex Newton, Principal
- ▲ Jane Richardson, Senior Vice Principal
- ▲ Paul Sutherland, Vice Principal
- ▲ Neil Kay, Vice Principal
- ▲ Leanne Madge, Assistant Principal
- ▲ Will Yeates, Assistant Principal
- ▲ Rhys Davies, Director of Sixth Form

Heads of Year

- ▲ Michaela Dorrian, Head of Year 7
- ▲ Duncan Smillie, Head of Year 8
- ▲ Charlotte Faulkner, Head of Year 9
- ▲ Sean Kirby, Assistant Head of Year 9
- ▲ Mel Taylor, Head of Year 10
- ▲ Darren Veale, Head of Year 11

Pastoral Support Managers

- ▲ Charlotte Fisk, PSM Year 7
- ▲ Nicola Bertram, PSM Year 8
- ▲ Tracey Pike, PSM Year 9
- ▲ Nathan Moore, PSM Year 10
- ▲ Donna Pearson, PSM Year 11
- ▲ Tracey Tunnard, Assistant Head of Sixth Form

Other Staff

- ▲ Amanda Woodcock, Administration Manager
- ▲ James Stanley, Network Manager

Appendix 3 CCTV User Rules

The following guidance is issued to all authorised users:

The College is permitted to record images for legitimate purpose and there are some simple rules which will keep us legal and safe.

We are allowed to capture images relating to the control and management of the College and we can view these images for this purpose. This covers behaviour management and site security.

However, the viewing of images must be supervised by an authorised person who should ask, "Is there a legitimate reason, relating to the College, why I (or anyone else asking to see the images) should be viewing these images?"

Examples of legitimate reasons:

- ▲ Behaviour management
- ▲ Investigating vandalism
- ▲ Investigating theft
- ▲ Safeguarding

Examples of possible legitimate reasons:

- ▲ Complaints by staff about other members of staff

Examples of non-legitimate reasons:

- ▲ Invasion of privacy
- ▲ Attempts to obtain personal data using images
- ▲ Voyeurism

In the case of the latter two categories, any requests that appear to fall into this category should be referred to the Responsible Person (Tony Jordan).

Any complaints about staff should be referred to the Principal.

It is inevitable that we also capture images of activity not related to college business and we need to be more careful in how we treat these images. For example, we capture images of members of the public walking past the college, parking in the car park etc. Requests to view any images such as this should be referred to the Responsible Person (Tony Jordan) before images are viewed.

Images may be preserved (*i.e. recording made*) e.g. if this is necessary for a disciplinary investigation. Only the Responsible Person or the Principal can authorise the recording of images.

The College must take good care of the images since this is personal data and so should not allow casual viewing by 'disinterested' staff or visitors. For this reason, the monitors should be switched off when not in use.

The College has adopted a Policy with regard to dealing with requests from persons who wish to view images of themselves or their children. This Policy is available from Data Protection Officer and must be followed.

It is not appropriate to use the images for amusement.