Pin Point Recruitment CCTV policy

Policy summary

Pin Point Recruitment has in place a Closed-Circuit Television (CCTV) surveillance system. This policy details the purpose, use and management of the CCTV system and details the procedures to be followed in order to ensure that Pin Point Recruitment complies with relevant legislation and Codes of Practice where necessary.

This policy and the procedures therein detailed, applies to all of the Pin Point Recruitment branch CCTV systems including covert installations capturing images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals. CCTV images are monitored and recorded in strict accordance with this policy.

Contents

Introduction

1. Pin Point Recruitment uses closed circuit television (CCTV) images for the prevention, identification and reduction of crime and to monitor the company offices in order to provide a safe and secure environment for staff and visitors and to prevent the loss of or damage to Pin Point Recruitment contents and property.
2. The CCTV system is owned by Pin Point Recruitment and managed by the IT Director. The IT Director is the system operator, and data controller, for the images produced by the CCTV system.
3. The CCTV system is operational and is capable of being monitored for 24 hours a day, every day of the year.

Purpose

4. This Policy governs the installation and operation of all CCTV cameras at all of the branches which operate for Pin Point Recruitment.
5. CCTV surveillance is used to monitor and collect visual images for the purposes of:
    - protecting the buildings and assets, both during services or office hours, and after hours.
    - promoting the health and safety of staff 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 the rules are respected so that the site/s can be effectively managed.

Scope

6. This policy applies to Pin Point Recruitment which occupy premises controlled by the CCTV system.
7. Where a system is jointly owned or jointly operated, the governance and accountability arrangements are agreed between the partners and documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and procedures for the resolution of any differences between the parties or changes of circumstance.
8. This policy is applicable to and must be followed by all staff including consultants. Failure to comply could result in disciplinary action, including dismissal.
9. All staff involved in the operation of the CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.
10. All systems users with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will have relevant skills and training on the operational, technical and privacy considerations and fully understand the policies and procedures.

Definitions

CCTV – closed circuit television camera. A TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes and where access to their content is limited by design only to those able to see it.

Data controller - the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of CCTV images.

Data Protection Act 2018 (DPA) - UK data protection framework, regulating the processing of information relating to individuals.

General Data Protection Regulations 2016 (GDPR) - European Union data protection framework, regulating the processing of information relating to individuals.

ICO CCTV Code of Practice 2017 - recommendations on how the legal requirements of the Data Protection Act 1998 can be met when using CCTV, issued by the Information Commissioner's Office. The guidance will be updated to comply with current legislation.

Security Industry Authority (SIA) - the organisation responsible for regulating the private security industry in the UK, under which private use of CCTV is licensed. It is an independent body reporting to the Home Secretary, under the terms of the Private Security Industry Act 2001.

Surveillance Camera Code of Practice 2013 - statutory guidance on the appropriate and effective use of surveillance camera systems issued by the Government in accordance with Section 30 (1) (a) of the Protection of Freedoms Act 2012.

System Operator - person or persons that take a decision to deploy a surveillance system, and/or are responsible for defining its purpose, and/or are responsible for the control of the use or the processing of images or other information obtained by virtue of such system.

System User - person or persons who may be employed or contracted by the system operator who have access to live or recorded images or other information obtained by virtue of such a system.

Policy

Policy statement

11. Pin Point Recruitment will operate its CCTV system in a manner that is consistent with respect for the individual's privacy.
12. Pin Point Recruitment complies with Information Commissioner's Office (ICO) CCTV Code of Practice 2017 to ensure CCTV is used responsibly and safeguards both trust and confidence in its continued use.
13. The CCTV system will be used to observe the areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.
14. The use of the CCTV system will be conducted in a professional, ethical, and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy.

15. Cameras will be sited so they only capture images relevant to the purposes for which they are installed. In addition, equipment must be carefully positioned to:
    - cover the specific area to be monitored only.
    - keep privacy intrusion to a minimum.
    - ensure that recordings are fit for purpose and not in any way obstructed (e.g., by foliage).
    - minimise risk of damage or theft.
16. CCTV will **not** be used for the purposes of streaming live services.

Location and signage

17. Cameras are sited to ensure that they cover the premises as far as is possible. Cameras are installed throughout the Pin Point Recruitments offices.
18. The location of equipment is carefully considered to ensure that images captured comply with data protection requirements. Every effort is made to position cameras so that their coverage is restricted to the Pin Point Recruitment offices, which may include outdoor areas.
19. Signs are placed within all offices in order to inform staff, visitors, and members of the public that CCTV is in operation.
20. The signage indicates that monitoring and recording is taking place, for what purposes, the hours of operation, who the system owner is and where complaints/questions about the systems should be directed.
21. Signage templates are included in Appendix 1.

Monitoring and recording

22. Cameras are monitored in a secure private office,
23. Images are recorded on secure servers and are viewable by the IT Director. Additional staff may be authorised by the IT Director to monitor cameras sited within their own areas of responsibility on a view only basis.
24. Where company offices are using Cloud-based storage they will ensure that such storage is located in the European Economic Area (EEA), and that all relevant security and data protection measures are in place.
25. Recorded material will be stored in a way that maintains the integrity of the image and information to ensure that metadata (e.g., time, date, and location) is recorded reliably, and compression of data does not reduce its quality.
26. Viewing monitors should be password protected and switched off when not in use to prevent unauthorised use or viewing.
27. The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked daily to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.
28. All images recorded by the CCTV System remain the property and copyright of the Pin Point Recruitment.

Covert surveillance

29. Covert surveillance is the use of hidden cameras or equipment to observe and/or record the activities of a subject which is carried out without their knowledge.
30. The Pin Point Recruitment will not engage in covert surveillance.

OR

33. The use of covert cameras will be restricted to rare occasions, when a series of criminal acts have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of the Company Directors will be sought before the installation of any covert cameras. The Company Directors should be satisfied that all other physical methods of prevention have been exhausted prior to the use of covert recording.

34. Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented and will only take place for a limited and reasonable period.

35. Where covert surveillance is authorised, its use must cease as soon as any active investigation has concluded.

Facial Recognition

36. Where cameras are used to identify people's faces, Pin Point Recruitment will ensure that we use high quality cameras to make sure we are capturing the individual accurately enough to fulfil the intended purpose. The results of this automatic matching will be monitored by a trained individual to ensure that there have not been any mismatches.
37. Any use of such automated technologies must involve some level of human interaction and should not be done on a purely automated basis.

Live Streaming

38. CCTV is not suitable for live streaming of services, as it is intended solely for safety and security purposes.

Data Protection

40. In its administration of its CCTV system, Pin Point Recruitment complies with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and in accordance with the Pin Point Recruitment Data Protection Policy.

Data Protection Impact Assessments

41. The CCTV system is subject to a Data Protection Impact Assessment. Any proposed new CCTV installation is subject to a Data Protection Impact Assessment identifying risks related to the installation and ensuring full compliance with data protection legislation. This will include consultation with relevant internal and external stakeholders.

42. Where existing CCTV systems are in operation as of May 2018, Pin Point Recruitment will endeavour to conduct a full Data Protection Impact Assessment on any upgrade or replacement of the system or within a 3-year period from the date of the implementation of GDPR, whichever is sooner.

Applications for disclosure of images

43. Requests by individual data subjects for images relating to themselves via a Subject Access Request should be submitted to the IT Director together with proof of identification. Further details of this process can be obtained by contacting the IT Director.
44. In order to locate the images on the system sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.
45. Where Pin Point Recruitment is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.
46. A request for images made by a third party should be made to the IT Director.
47. In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.
48. Such disclosures will be made at the discretion of the Company Directors with reference to relevant legislation and where necessary.
49. Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager, the IT Director may provide access to CCTV images for use in staff disciplinary cases.
50. A log of any disclosure made under this policy will be held by IT Director itemising the date, time, camera, requestor, reason for the disclosure; requested; lawful basis for disclosure; date of decision and/or release, name of authoriser.
51. Before disclosing any footage, consideration should be given to whether images of third parties should be obscured to prevent unnecessary disclosure.
52. Where information is disclosed, the disclosing officer must ensure information is transferred securely.
53. Images may be released to the media for purposes of identification. Any such decision to disclose will be taken in conjunction with the Police and/or other relevant law enforcement agencies.
54. Surveillance recordings must not be further copied, distributed, modified, reproduced, transmitted, or published for any other purpose.

Retention of images

55. Unless required for evidentiary purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than thirty-one calendar days from

the date of recording. Images will be automatically overwritten or destroyed after this time.

56. Where an image is required to be held in excess of the retention period the IT Director will be responsible for authorising such a request, and recordings will be protected against loss or held separately from the surveillance system and will be retained for 6 months following date of last action and then disposed of.
57. Images held in excess of their retention period will be reviewed on a three-monthly basis and any not required for evidentiary purposes will be deleted.
58. Access to retained CCTV images is restricted to the IT Director and other persons as required and as authorised by the Company Directors.

Complaints Procedure

59. Complaints concerning the Pin Point Recruitment use of its CCTV system, or the disclosure of CCTV images should be made to the IT Director.
60. When requested, anonymised information concerning complaints will be provided to the Company Directors.

Review Procedure

61. There will be an annual review of the use of the CCTV system to ensure it remains necessary, proportionate, and effective in meeting the stated purposes.
62. As part of the review Pin Point Recruitment will assess:
    - whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.
    - the monitoring operation, e.g., if twenty-four monitoring in all camera locations is necessary or whether there is a case for reducing monitoring hours.
    - whether there are alternative and less intrusive methods for achieve the stated purposes.

Responsibilities

63. The IT Director is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring, and ensuring compliance with this policy.
64. The IT Director is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.
65. The IT Director is responsible for authorising the disclosure of images to data subjects and third parties and for maintaining the disclosure log.

Approval and review

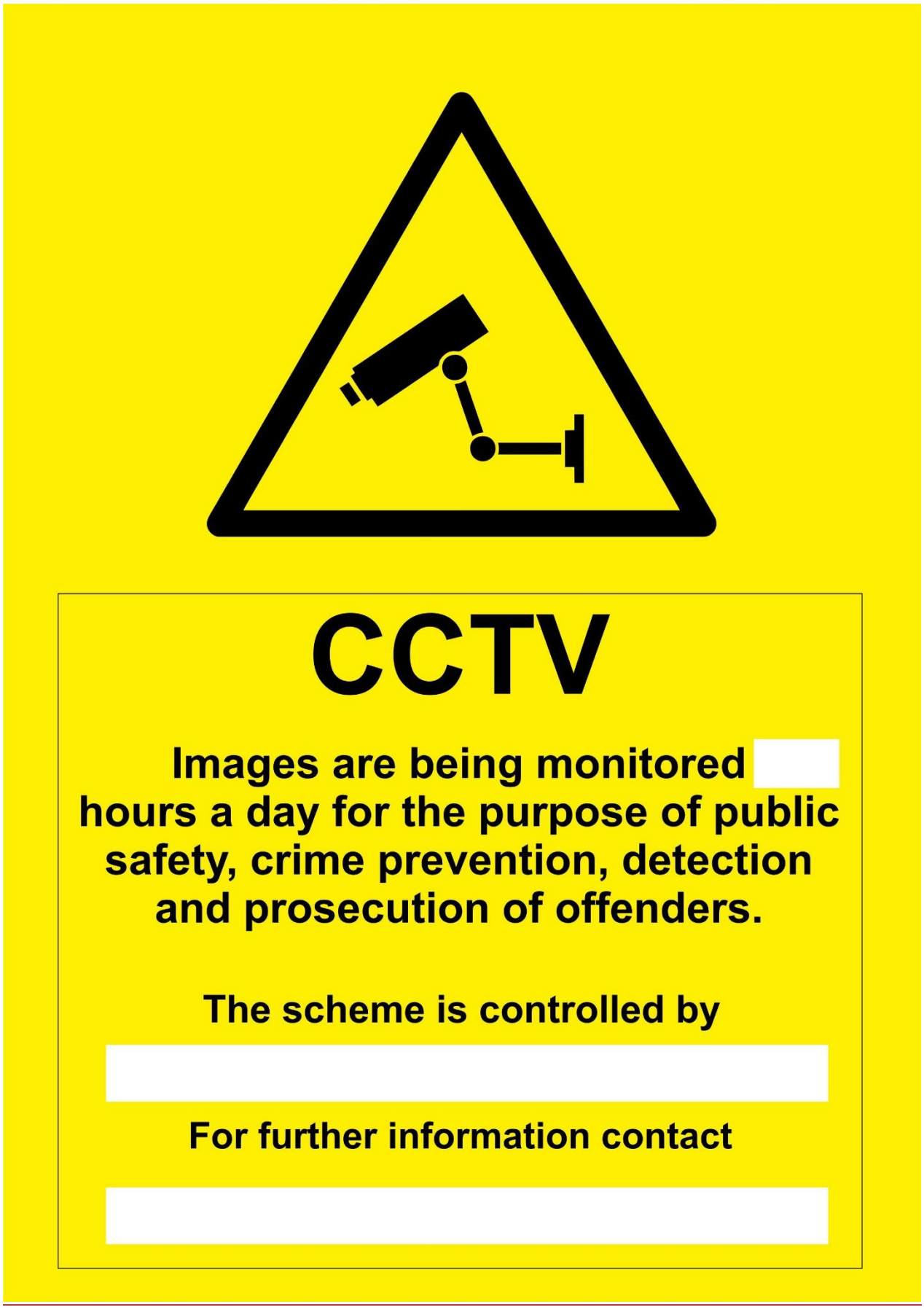
Approved by	
Policy owner	
Policy author	T Carney, IT Director, Pin Point Recruitment
Date	29/04/2022
Review date	

Revision history

Version no.	Revision date	Previous revision date	Summary of changes
0.1			Draft CoE CCTV Policy Template

Appendix 1 – CCTV Template Signage


CCTV
Images are being monitored for the purpose of public safety, crime prevention, detection and presecution of offenders.
The scheme is controlled by
For further Information contact


CCTV
Images are being monitored
hours a day for the purpose of public safety, crime prevention, detection and prosecution of offenders.
The scheme is controlled by
For further information contact