CCTV POLICY

1. INTRODUCTION

Stephens Scown LLP ("we", "us", "our" or "the Firm") have a continuing commitment to protecting and respecting your personal data and privacy.

This policy is in relation to our use of CCTV (as defined in this policy). Which we believe plays a legitimate and substantial role in helping to maintain a safe and secure environment for all our staff and visitors. We have designed this policy in order to address any concerns that may arise about the effect our collection of data through CCTV may cause.

The images recorded by our surveillance systems are classed as personal data which, must be processed in accordance with Data Protection Laws as defined bellow. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, relating to their personal data, is recognised and respected throughout the firm.

2. KEY DEFINITIONS

2.1. The following definitions apply in this policy:

CCTV	Any and all cameras designed to capture and record images of individuals and property.
Data	The information, which is stored electronically, or in certain paper-based filing systems. In respect of CCTV this will generally means video images. This may also include static pictures such as printed screen shots.
Data controllers	The people who, or the organisation which, determines the manner in which any personal data is to be processed. They are responsible for establishing practices and policies to ensure compliance with the data protection laws.
Data processors	Any person or organisation that is not a data controller (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions.
Data Protection laws	To mean all relevant data protection legislation including but not limited to; the Data Protection Act 1998 and 2018 (DPA), The UK General Data Protection Regulation (UK GDPR) together, and with other subsequent laws passed to bring the UK GDPR into effect in England and Wales after 31 December 2020 "Data Protection Laws".
Data subject	All living individuals who can be identified from that data (or other data legally in our possession). This includes any and all video images of identifiable individuals.
Data users	Our employees whose work involves the processing of personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor,

	store, retrieve and delete images. All data users must handle data in accordance with this policy and our Privacy Policy.
ICO	Information commissioner's office – the ICO is the independent regulatory office dealing with the implementation of data protection laws in the United Kingdom.
Privacy policy	A policy detailing how we will process a data subjects information. Our privacy policy is available at: https://www.stephens-scown.co.uk/legal-notices/privacy-statement/
Processing	Any and all activity which involves the use of data. This includes the obtaining, recording or holding of data, or carrying out any operation on the data including organising, amending retrieving, using, disclosing or destroying it.
Surveillance systems	To mean any device or system designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition, body worn cameras, unmanned aerial systems and any other system that is able to be used to capture information of identifiable individuals or information relating to identifiable individuals.

3. WHO ARE WE AND HOW TO CONTACT US

3.1. For the purpose of the Data Protection Laws, the Data Controller is Stephens Scown LLP, registered company number OC356696. If you want to request more information about our Privacy Policy or information regarding data protection you should contact us using the details provided below:

FAO: Privacy Officer

Address: Curzon House, Southernhay West, Exeter, Devon, EX1 1RS

Email: privacyofficer@stephens-scown.co.uk

Telephone: 01392 210700 and ask to speak to the Governance and Privacy Officer.

4. ABOUT THIS POLICY

4.1. We use CCTV for the purpose of viewing and recording individuals on and around our premises. This policy is designed to outline why we use CCTV, how we will use CCTV and the ways we will process the data recorded by CCTV to ensure compliance with Data Protection Law and practice. This policy also explains how individuals can make a subject access request in respect of personal data created by CCTV.

4.2. We acknowledge that information that we hold about individuals is subject to the Data Protection Laws. The images of individuals recorded by CCTV cameras in the workplace are classified as personal data and therefore subject to the Data Protection

Laws. We are committed to complying with all our legal obligations and seek to comply with suggestions from the ICO's interpretation of the regulations.

4.3. This policy covers both employees (including but not limited to; partners, directors, associates, consultants, contractors, freelancers, volunteers, interns, casual workers, zero hour workers, and agency workers) and all visiting members of the public (including clients).

4.4. This policy is non-contractual and does not form part of any terms and conditions of any employment or other contractual agreement. We may amend this policy at any time without consultation. This policy will be regularly reviewed to ensure that it matches the legal requirements, along with all relevant guidance published by the ICO and/or industry standards.

4.5. A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following an investigation, a breach of this policy may be regarded as misconduct; leading to disciplinary action, up to and including dismissal. We may report any breach of criminal legislation to the appropriate authority.

5. PERSONNEL RESPONSIBLE

5.1. The Risk and Compliance Board has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the Governance and Privacy Officer. Day-to-day operational responsibility for CCTV and the storage of data recorded is the responsibility of the Facilities manager.

5.2. The responsibility for keeping this policy up to date has been delegated to the Governance and Privacy Officer.

6. VALID LAWFUL BASIS

6.1. The Firm has ratified that the use of CCTV is necessary for the legitimate business interests of the firm, for the purposes listed below;

a) To prevent crime and protect our buildings and assets from damage, disruption, vandalism and other acts of crime;
b) For the personal safety of staff, visitors and other members of the public and to also act as a deterrent against crime;
c) To support law enforcement bodies in the prevention, detection and prosecution of crimes;
d) To assist in the day-to-day management, including ensuring the health and safety of staff and others around our premises;
e) To assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;
f) To assist in the defence of any civil litigation, including employment tribunal proceedings; and

g) For other business/site specific purposes.

The above list is not extensive or exhaustive and other purposes and valid lawful basis may be relevant in the course of our business operations.

7. MONITORING

7.1. CCTV monitors the exterior and interior of our buildings, all client areas (excluding meeting rooms) and specifically reception, events rooms, and main entrances of those buildings including carparking areas. This monitoring will be 24 hours a day 365 days' a year, and this data is continuously recorded.

7.2. Our camera locations have been chosen to minimise views of spaces not relevant to their legitimate purpose. As far as is practically possible, our CCTV cameras will not focus on private homes, gardens or other areas of private property.

7.3. Surveillance systems will not be used to record sound.

7.4. Images are monitored by authorised personnel only.

7.5. Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of data.

8. HOW WE WILL OPERATE ANY CCTV

8.1. Where CCTV cameras are placed in the workplace we will ensure that signs are displayed at the entrance of the surveillance zone(s) to alert individuals that their image may be recorded. Such signs will contain details of the organisations operating the system, the purpose for using the surveillance system and who to contact for further information.

8.2. Live feeds from CCTV cameras will only be monitored where and when we deem this necessary.

8.3. We will ensure that both live feeds from cameras and recorded images are only viewed by approved members of staff, whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure locations.

9. USE OF DATA GATHERED BY CCTV

9.1. In order to ensure that the rights of the individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that allows for the maintaining of integrity and security for all parties involved.

9.2. Given to the large amounts of data generated by a surveillance system, we may chose to store video footage using a cloud based computing system. We will ensure that all reasonable steps are made to make sure that any cloud based service provider maintains the security of our information, in accordance to both regulatory and industry standards.

9.3. We may engage data processors to process data on our behalf. During this instance (if/when it becomes relevant) we will ensure reasonable contractual obligations are in place to safeguard the security and integrity of the Data Subject's information.

In limited circumstances images may be requested by law enforcement.
In limited circumstances images may be requested for insurance purposes.

10. **RETENTION AND ERASURE OF DATA GATHERED BY CCTV**

10.1. The data recorded by the CCTV will be stored while relevant; however, said data will not be retained indefinitely. It will be permanently deleted once there is no reasonable ground to retain the recorded information. Exactly how long these video images shall be retained for will vary according to the purpose for which they were recorded in the first instance.

10.2. At the end of their useful/reasonable life, all images stored in whatever format will be erased permanently and securely in line with the Firms Retention Policy. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

11. **USE OF ADDITIONAL SURVEILLANCE SYSTEMS**

11.1. Prior to introducing any/all new surveillance systems, including placing of a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a privacy impact assessment (PIA).

11.2. A PIA will be used to assist the Firm in deciding whether or not a new surveillance system is necessary and proportionate to the circumstances. The PIA will determine whether the system should be used and whether or not any limitations should be placed on the system.

11.3. PIAs consider the nature of the problem that we are seeking to address and whether the surveillance camera is likely to be an effective solution. In particular, we will consider the effect a surveillance camera will have on individual’s rights and therefore whether the use of surveillance is proportionate to the problems identified.

11.4. No surveillance cameras will be placed in areas where there is an expectation of privacy unless, in the most exceptional of circumstances, when it is judged by us to be necessary.

12. **COVERT MONITORING**

12.1. The Firm will never normally engage in the action of covert monitoring or surveillance on individuals. Covert monitoring is defined as the process of monitoring individuals who are unaware such actions are taking place.

12.2. Covert monitoring will only occur in highly exceptional circumstances, where there are considerable grounds to suspect criminal activity or serous malpractice is taking place.

12.3. 'The Firm' will only take this action after suitable consideration and in the belief that there is a no less intrusive way to address the perceived issue.

12.4. In the unlikely event that covert monitoring is deemed to be justified, it can/will only be carried out with the express authorisation of the Risk and Compliance Board.

12.5. Limited numbers of people will be aware of or involved in any practice involved in covert monitoring.

12.6. Covert monitoring when deemed justified will only be carried out for a limited and reasonable period of time consistent with the objectives laid out by the Firm. Also this recording will only relate to the specific suspected illegal or unauthorised activity.

13. **ONGOING REVIEW**

13.1. We will conduct periodic evaluations of the use of CCTV cameras in the workplace. This is to ensure that the use of this policy remains appropriate and necessary for its function, and that any surveillance system is continuing to address the needs that justified its initial introduction.

14. **DATA SUBJECT RIGHTS; COMPLAINTS AND GENERAL**

14.1. This policy is subject to our Privacy Statement.

If you have any queries or suggested amendments to this document, please contact:

Contact Name	Robert Brooks – Governance and Privacy Officer
E-mail	privacyofficer@stephens-scown.co.uk
Tel	01392 210700
Date/Version	11 December 2025 Version 1.a