1. INTRODUCTION

1.1. This CCTV Policy applies to the West Group Limited and The West Group USA, Inc (together referred to as "we", "us", "our"). It governs the use of CCTV systems operated at our premises and the processing of Personal Data captured through those systems.

1.2. Our Data Protection Officer (DPO) has overall responsibility of overseeing effective implementation, operation, and review of this CCTV Policy.

1.3. All employees, contractors and visitors are expected to comply with this Policy when working for, visiting, or otherwise acting on our behalf. This Policy should be read alongside our Data Privacy Policy.

Any queries in relation to this Policy should be directed to the **Data Protection Officer** at DPO@westgroup.co.uk for both the UK and US.

2. ABOUT THIS NOTICE

2.1. We currently use CCTV to record and view areas and activity which may include individuals in specified locations in and around our premises located at:

COMPANY NAME	COMPANY ADDRESS
The West Group Limited	29 Aston Road, Waterlooville, Hampshire PO7 7XJ
The West Group Limited	19 Arnside Road, Waterlooville, Hampshire PO7 7UP
The West Group Limited	43-44 Aston Road, Waterlooville, Hampshire, PO7 7XJ
The West Group Limited	7 Waterberry Drive, Waterlooville PO7 7UW
The West Group USA, Inc	2360 Crist Road, Suite B800, Garland, Texas, 75040

2.2. We have carried out a Data Privacy Impact Assessment to ensure we are balancing our need for CCTV with the impact on the privacy of Data Subjects.

2.3. This Policy outlines why we use CCTV, how we will use CCTV and how we will process Data recorded by CCTV to ensure it is compliant with applicable Data Protection Laws. It will also explain how to make a Data Subject Request in respect of Personal Data created by CCTV.

2.4. We may update this Policy from time to time. Any material changes will be communicated on our website and will be effective immediately after such notification.

2.5. Where CCTV footage is accessed or stored across jurisdictions, appropriate safeguards are applied in accordance with applicable Data Protection Laws, including, where required by UK GDPR ("UK GDPR", meaning the UK General Data Protection Regulation), the use of a UK International Data Transfer Agreement ("UK International Data Transfer Agreement" or "IDTA", meaning the standard contractual clauses approved by the UK Information Commissioner's Office for international data transfers) or equivalent approved transfer mechanism and US data protection laws.

3. DEFINITIONS

For the purposes of this Policy, the following terms have the following meanings:

CCTV: means fixed and domed cameras designed to capture and record images of individuals and property.

Data: means information, which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data Subjects: means all living individuals about whom we hold Personal Data as a result of the operation of our CCTV (or other surveillance systems).

Personal Data: means Data relating to a living individual who can be identified from that Data (or other Data in our possession). This will include video images of identifiable individuals.

Data Controllers: means people or organisation which determine the way any Personal Data is processed. They are responsible for establishing practices and policies to ensure compliance with Data Protection Laws. The West Group Limited and The West Group USA, Inc. are the Data Controllers of all Personal Data collected through our CCTV systems.

Data Users: means our employees whose work involves processing 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. Data Users must protect the Data they handle in accordance with this Policy and our Data Protection Policy.

Data Processors: means a person or organisation that is not a Data user (or other employee of a Data Controller) that processes Data on our behalf and in accordance with our instructions (for example, a supplier which handles Data on our behalf).

Data Protection Laws: means UK General Data Protection Regulation, the Data Protection Act 2018, and applicable US federal and Texas state privacy laws and applicable regulatory guidance.

Processing: means any activity which involves the use of Data. It includes obtaining, recording, or holding Data, or carrying out any operation on the Data including organising, amending, retrieving, using, disclosing, retaining, or destroying it. Processing also includes transferring or transmitting personal Data to third parties, whether within or outside the United States or the United Kingdom.

Surveillance Systems: means any device or systems designed to monitor or record images of individuals or information relating to individuals. We do not currently use facial recognition or biometric identification through CCTV. We do not routinely use audio recording through CCTV.

4. REASONS FOR THE USE OF CCTV

4.1. We currently use CCTV as outlined below. Such use is necessary and proportionate for the following legitimate business purposes, and we have conducted a balancing test to ensure our legitimate interests do not override the rights and freedoms of Data Subjects:

a) to prevent crime and protect buildings and assets from damage, disruption, vandalism, and other crime.

b) for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime.

c) to support law enforcement bodies in the prevention, detection, investigation, and prosecution of crime, in accordance with applicable legal requirements and Data Protection Laws

d) to assist in day-to-day management, including ensuring the health and safety of staff and others.

e) to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings, subject to applicable employment laws and Data Protection Laws.

f) to assist in the defence of any civil litigation, including health and safety incidents and accidents.

4.2. This list is not exhaustive, but such use will be limited to cases where strictly necessary and proportionate. We may use CCTV for other purposes where we have a legitimate business need and where such use is consistent with applicable law and the reasonable expectations of individuals being monitored.

5. MONITORING

5.1. CCTV is used to monitor the exterior of the buildings, including main entrances and secondary exits. Where installed, CCTV may also monitor limited areas within the interior of certain premises, such as reception areas or manufacturing floors.

5.2. CCTV footage is recorded continuously. Live monitoring is limited to authorised Data Users during working hours except in emergency situations where monitoring outside of working hours may be necessary for security purposes.

5.3. Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property. In compliance with Texas Penal Code 21.15, applicable federal law, UK GDPR, and the ICO's CCTV Code of Practice, surveillance cameras will never be installed or positioned to capture images or audio in areas where individuals have a reasonable expectation of privacy, including but not limited to toilets, locker rooms, changing rooms, shower facilities, private offices and meeting rooms where confidential discussions occur, nursing mothers' rooms, or areas designated for lunch breaks.

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

6. HOW WE WILL OPERATE ANY CCTV

6.1. Where CCTV cameras are placed in the workplace or on our premises, we will ensure that clear and conspicuous signs are displayed at all entrances and at the boundary of each surveillance zone to alert individuals that video surveillance is in use and whether audio recording is enabled. The signs will be visible, easy to read and will contain a statement that video surveillance and/or audio recording is in use, the name of the organisation operating the system and the purpose for using the surveillance system.

6.2. We will ensure that live feeds from cameras and recorded images are only viewed by authorised Data Users 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 offices.

7. USE OF DATA GATHERED BY CCTV

7.1. In order to ensure that the rights of individuals recorded by CCTV systems are protected, we will ensure that Data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the Data where it is possible to do so.

7.2. We may engage Data Processors to process Data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the Data.

8. RETENTION, ERASURE AND SECURITY BREACH NOTIFICATION OF DATA GATHERED BY CCTV

8.1. Data recorded by the CCTV system will be stored. Data from CCTV cameras will not be retained indefinitely but will be overwritten on a rolling basis, approximately every 30 days.

8.2. At the end of their useful life, all images stored in whatever format will be erased permanently and securely. 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.

8.3. In the event of a breach of system security that compromises Data from the CCTV containing Personal Data, we will provide notification to affected individuals as quickly as possible and in compliance with Texas Business and Commerce Code Section 521.053 and applicable data protection laws. Notification timing will not be delayed except as necessary to: (i) determine the scope of the breach and restore the reasonable integrity of the data system, or (ii) comply with lawful requests from law enforcement to delay notification where such notification would impede a criminal

investigation. Where direct notification to affected individuals is possible, notification will include: (a) the date or estimated date of the breach; (b) a description of the Personal Data that was acquired or reasonably believed to have been acquired; (c) contact information for the individual to obtain further information, including a telephone number, email address, and postal address; (d) a general description of our response and remedial measures; and (e) information about what steps the affected individual can take to protect themselves from potential harm. Where required by applicable law, we will notify the Texas Attorney General's Office of any breach affecting more than 10,000 Texas residents and will notify any other appropriate law enforcement or regulatory authority, including the Federal Trade Commission. Where a breach affects Personal Data subject to UK data protection law, we will notify the Information Commissioner's Office within the applicable statutory timeframe (where feasible) and will notify affected individuals without undue delay where there is a high risk to their rights and freedoms.

9. AUDIO RECORDINGS

9.1. Some of our surveillance systems have the technical capability to capture audio recordings. Audio recording is not routinely enabled or used. Where it is considered necessary to enable audio recording, this will be done only where strictly required for the legitimate purposes set out in section 4 of this Policy and in compliance with Texas Penal Code Section 16.02, the Investigatory Powers Act 2016, and all other applicable laws including UK GDPR.

9.2. Before enabling audio recording capabilities, we will: (a) carry out a Data Protection Impact Assessment and ensure a documented lawful basis for audio recording; (b) make this Policy available to employees, visitors and other relevant individuals and (c) display clear and prominent signage at all entrances and monitored areas indicating that audio recording is in use. We will not enable audio recording in areas where individuals have a reasonable expectation of privacy.

9.3. We follow the same rules as for CCTV footage regarding Data capture, downloading and sharing with third parties. When downloaded, we keep the Data for legitimate purposes and in accordance with Data Protection Laws.

10. REQUESTS FOR DISCLOSURE

10.1. We may share Data with any company in our group and other organisations in accordance with applicable Data Protection Laws and regulations, where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 4.1. When sharing Data with third parties, we will implement appropriate safeguards through written agreements requiring such parties to maintain the confidentiality and security of Personal Data and to process it only for the specified purposes.

10.2. No images or audio recordings from our CCTV cameras will be disclosed to any third party without express written permission being given by the Data Protection Officer, the Group IT Administrator, or

other authorised senior manager. Data will not be released unless: (a) required by a valid court order, subpoena, or other legal process; (b) required for legal proceedings and the requesting party has provided satisfactory evidence of such requirement; or (c) otherwise required by applicable law. We reserve the right to challenge any request we believe to be invalid, overly broad, or not legally enforceable.

10.3. In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime, provided that: (a) the request is made in writing; (b) the requesting agency provides adequate identification and authority; (c) the request specifies the footage sought with reasonable particularity; and (d) we document the disclosure in accordance with paragraph

10.4. We will maintain a written record, in both electronic and physical format with appropriate security controls and access restrictions, of all disclosures of CCTV footage, including: (a) the date and time of disclosure; (b) the identity of the recipient; (c) the purpose of the disclosure; (d) a description of the footage disclosed; (e) the legal basis or authorisation for the disclosure; and (f) the identity of the person authorising the disclosure; and (g) where the recipient is a member of the public, documentation of identity verification procedures undertaken prior to disclosure. Such records shall be retained for a minimum of six (6) years from the date of disclosure, or for such longer period as may be required by applicable law, legal hold obligations, or pending litigation or regulatory investigations. In the event of any data subject access request, complaint, or regulatory inquiry related to a disclosure, the associated records shall be retained until final resolution of such matter plus an additional two (2) years.

10.5. No images from CCTV will be posted online or disclosed to the media, except where: (a) required by law or court order; (b) necessary to assist in the detection or prosecution of serious crime with prior written authorisation from the Data Protection Officer and appropriate consultation with law enforcement; or (c) the Data Subject has provided specific, informed written consent for such disclosure.

11. DATA SUBJECT ACCESS REQUESTS

11.1. In certain circumstances, Data Subjects may make a request for disclosure of their Personal Data, and this may include CCTV images (“Data Subject Access Request”). A Data Subject Access Request must be made in writing to the Data Protection Officer and is subject to the statutory conditions and procedures under applicable Data Protection Laws. We will respond to such requests within the timeframes required by applicable law.

11.2. To enable us to locate relevant footage efficiently, any requests for copies of recorded CCTV images should include: (a) the approximate date and time of the recording; (b) the specific location where the footage was captured; and (c) information sufficient to identify the individual in the footage. If a request lacks sufficient detail to enable us to locate the footage using reasonable efforts, we will inform the requestor and provide them with an opportunity to provide additional information. We are

not obliged to conduct unreasonably burdensome searches for footage that cannot be identified with reasonable specificity.

11.3. We reserve the right to redact or obscure images of third parties when disclosing CCTV Data as part of a subject access request, where necessary to protect the rights and freedoms of such third parties, provided that such redaction does not prevent the requestor from exercising their access rights. We will apply the minimum redaction necessary to achieve this purpose.

12. REQUESTS TO PREVENT PROCESSING

12.1. We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making. For further information regarding these rights and other rights, please contact the Data Protection Officer.