

# CCTV POLICY & PROCEDURES

## Contents

1. INTRODUCTION .....	2
2. SCOPE .....	2
3. OBJECTIVES .....	2
4. OPERATION OF THE CCTV SURVEILLANCE SYSTEM .....	2
5. MONITORING OF CCTV IMAGES .....	2
6. RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS .....	3
Access to Recordings by Staff or Third Parties.....	3
7. COMPLAINTS/BREACHES .....	4
8. RESPONSIBLE OFFICER .....	4
9. MONITORING AND REVIEW .....	4
10. POLICY REVIEW .....	4

To support Information Security Policy Framework

## 1. INTRODUCTION

These procedures are applicable to all QRS staff. Their purpose is to ensure that the Closed Circuit Television (CCTV) system is used to create a safer environment for staff and visitors to ensure that its operation is consistent with the Data Protection Principles which are set out in the General Data Protection Regulation/Data Protection Act. For the purposes of the GDPR, the Data Controller is QRS Market Research Ltd.

QRS has installed a comprehensive CCTV system for the principal purposes of monitoring who is entering and exiting the building. In the unlikely event of a crime being committed, it will also be used for the purposes of preventing/detecting crime and promoting staff safety.

The images from the CCTV system are monitored by company Directors.

## 2. SCOPE

These procedures apply to both CCTV cameras and equipment on the premises. QRS Market Research Ltd is the Data Controller for this system and determines the purpose of recording and is legally responsible and accountable for its use.

## 3. OBJECTIVES

The CCTV surveillance system has been installed and is monitored for the following purposes:

- To assist in the prevention of crime and to aid safety

## 4. OPERATION OF THE CCTV SURVEILLANCE SYSTEM

### **The System**

The system is operational and images are capable of being monitored twenty-four hours a day throughout the year. All CCTV cameras are configured to record images only.

## 5. MONITORING OF CCTV IMAGES

The Information Security Director (Lee Tomlin) will ensure that all staff who have responsibility for the system are fully briefed and trained in respect to all functions, both operational and administrative, arising within the operation of CCTV surveillance, including training in the data security requirements of these procedures and the General Data Protection Regulation/Data Protection Act.

The control of the CCTV Surveillance System will always remain with the Directors. However, at the discretion of the Directors, we may act on advice from the police in order to operate cameras during an incident to assist in the detection of crime or facilitate the apprehension and prosecution of offenders in relation to crime and public order. On each occasion the Police are assisted with their operations, a report setting out the time, date and detail of the incident will be recorded and the original incident will be updated within the Safeguard system.

## 6. RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

All recording media used for the monitoring and capture of images on the QRS CCTV system belong to and remain the property of QRS.

Should it be necessary for images to be retained for release to a third party (including the Police) under the exemptions contained within the General Data Protection Regulation/Data Protection Act, or retained for any other purpose in accordance with these procedures, for which the Company's use of the system is registered with the Information Commissioner's Office, copies of those images will be transferred to a secure encrypted computer file. There will be a charge for any access request made, as per the current rates set out by the Information Commissioner's Office.

All media containing recordings will be securely destroyed at the end of their lifespans.

### Access to Recordings by Staff or Third Parties

It is important that access to and disclosure of images is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes.

Access to recorded images will be restricted to the Directors.

All requests by persons or organisations outside of the Company (including any bodies that may claim a statutory or legal right of access) for viewing or obtaining recordings must be assessed on a case by case basis by the IT/Information Security Director and the Data Protection Officer and the other relevant officers responsible for authorising the disclosure of staff personal data. Access will not be granted unless the responsible officers are satisfied that this is consistent with the obligations placed on the General Data Protection Regulation/Data Protection Act.

All requests for access will be recorded detailing:

- ⇒ the date, time and purpose of the request,
- ⇒ the decision to release or withhold the images and the reasons for the decision in each case,
- ⇒ the date and time at which access was allowed/or disclosure made;
- ⇒ the extent of the information accessed/disclosed;
- ⇒ the name and role of the member of staff making the decision to allow or withhold access,
- ⇒ the name of the staff member providing access.

If the IT/Information Security Director considers that the assistance of a member of staff is needed to identify a victim, witness or perpetrator in relation to a criminal incident, wherever practicable, the member of staff should be invited to view the images in a Directors office.

A police officer may request access to CCTV images held by QRS. In most cases the police will request such access in response to a request by QRS to investigate an alleged offence.

## 7. COMPLAINTS/BREACHES

Any concerns or complaints regarding the use of CCTV should, in the first instance, be addressed to the Data Protection Officer.

Concerns or queries relating to any aspect of compliance with General Data Protection Regulation/Data Protection Act should be directed to the Data Protection Officer.

## 8. RESPONSIBLE OFFICER

The IT/Information Security Director is responsible for the implementation of these procedures, in consultation with the Data Protection Officer.

## 9. MONITORING AND REVIEW

The IT/Information Security Director and the Data Protection Officer will monitor compliance with these procedures and the operational effectiveness of the Company CCTV system. They will initiate reviews of the procedure in the light of developments in the current legislation which underpins the procedures.

## 10. POLICY REVIEW

This policy is reviewed annually.

*These policies supplement your terms of employment but are not of contractual effect. Their purpose is to explain the Company's current policies and procedures, but they may be subject to change without notice if changes are considered appropriate by the Company or if there are changes in relevant legislation.*