CCTV POLICY

INTRODUCTION

This document sets out the appropriate actions and procedures which must be followed to comply with the Data Protection Act in respect of the use of CCTV (closed-circuit television) surveillance systems.

In drawing up this policy, due account has been taken of the following:

1. The Data Protection Act 2018
2. European Union General Data Protection Regulation 2016 (EU GDPR)
3. In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information, published by the Information Commissioner's Office
4. The Human Rights Act 1998
5. The Regulation of Investigatory Powers Act 2000
6. Caldicott Report 1997.

This policy should be read in conjunction with 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information', published by the Information Commissioner's Office.

SCOPE

This policy covers all employees and persons providing a service to the Company, visitors and all other persons whose image(s) may be captured by the system.

DEFINITIONS

Prior to considering compliance with the principles of the Data Protection Act, a user of CCTV or similar surveillance equipment will need to determine two issues:

The type of personal data being processed, i.e. is there any personal data which falls within the definition of **sensitive processing** as defined by the Act; 'Sensitive processing' includes:

1. Gender
2. Ethnic origin or race
3. Political opinion
4. Religious beliefs
5. Trade Union membership
6. Health – mental or physical
7. Sexual life
8. Commission of any offence (or alleged)
9. Any court proceedings or findings.

The **purpose(s)** for which both personal and sensitive personal data is being processed. The data must be:

1. Fairly and lawfully processed

2. Processed for limited purposes and not in any manner incompatible with those purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in accordance with individual's rights
7. Secure
8. Not transferred to countries without adequate protection.

The Information Commissioner will take into account the extent to which users of CCTV and similar surveillance equipment have complied with the Code of Practice when determining whether they have met their legal obligations when exercising their powers of enforcement.

POLICY APPLICATION
Initial Assessment Procedures

The Directors have the legal responsibility for the day-to-day compliance with the requirements of the CCTV Code of Practice.

The purpose of the CCTV Policy is for the prevention or detection of crime or disorder, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), interest of public and employee Health and Safety, protection of public health and the protection of the Company's property and assets.

Prior to any camera installation the Directors will ensure that the installation complies with the Data Protection Act and CCTV Code of Practice.

Siting the Cameras

It is essential that the location of the equipment be carefully considered, because the way in which images are captured will need to comply with the Data Protection Act.

All cameras are located in prominent positions within public and staff view and do not infringe on sensitive areas. All CCTV surveillance is automatically recorded and any breach of these Codes of Practice will be detected via controlled access to the system and auditing of the system.

Signs have been erected on all entrance points to Company premises and throughout the site to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment. The signs must include details on the purpose, organisation and contact details.

Use of Covert CCTV (Directed) surveillance if required should be requested through the Police. This is covered by the Regulation of Investigatory Powers Act 2000 (RIPA).

Quality of the Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme be clearly identified. For example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

All camera installations and service contracts should be undertaken by NACOSS approved security companies. Upon installation all equipment is tested to ensure that only the designated areas are monitored and high quality pictures are available in live and play back mode. All CCTV equipment should be serviced and maintained on an annual basis.

Processing the Images

Images which are not required for the purpose(s) for which the equipment is being used should not be retained for longer than is necessary. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images are controlled in accordance with the requirements of the Data Protection Act.

All images are digitally recorded and stored securely within the systems hard drives. Automatic erasure takes place after 31 days.

Where the images are required for evidential purposes or disciplinary proceedings, a CD-R disc recording is made and placed in a sealed envelope, signed and dated and held by the Directors until completion of the investigation. Viewing of images within the system is controlled by the Directors or a person nominated to act on their behalf. Only persons trained in the use of the equipment and authorised by the Directors can access data.

Access to and Disclosure of Images to Third Parties

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment are restricted and carefully controlled. This will ensure that the rights of individuals are preserved, but also to ensure that the continuity of evidence remains intact should the images be required for evidential purposes, e.g. a Police enquiry or an investigation being undertaken as part of the Organisation's disciplinary procedure.

Access to the medium on which the images are displayed and recorded is restricted to the Directors and third parties as authorised.

Access and disclosure to images are permitted only if this supports the purpose of the scheme. Under these conditions the CCTV images record book must be completed.

Access to Images by Individuals

The Data Protection Act gives any individual the right to request access to CCTV images.

Individuals who request access to images must be issued an access request form. Upon receipt of the completed form, the Directors and the Organisation's **Data Protection Officer** will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. If the duty of care cannot be discharged then the request can be refused.

A written response will be made to the individual, giving the decision (and if the request has been refused, giving reasons) within one calendar month of receipt of the enquiry. No payment is required, except under exceptional circumstances (e.g. an unreasonably large amount of data requested).

Interaction with other Policies and Procedures

This policy should be read in conjunction with the Organisation's Data Protection Policy.

Responsibilities

The Directors have responsibility for the implementation of this policy, monitoring its effectiveness and ensuring the CCTV Code of Practice is available to view.

The Organisation's **Data Protection Officer** is also personally accountable for ensuring that the policy and Code of Practice are adhered to and monitored.

Enforcement

The Information Commissioner has the power to issue Enforcement Notices where it is considers that there has been a breach of one or more of the Data Protection Principles. An Enforcement Notice would set out the remedial action that the Commissioner requires of the Organisation to ensure future compliance with the requirements of the Act.

Documentation

Copies of all documentation and records relating to the CCTV system will be held by the Directors.

Review

This policy will be reviewed within the Management Reviews of the Organisation's ISO/IEC 27001 Information Security Management System. This will be at intervals as determined by the ISMS Committee.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	15/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Updating dates