Outcomes First Group

CCTV Policy v5.1

Policy Folder: Data Protection

Outcomes First Group

CONTENTS Page

1.0 INTRODUCTION

The purpose of this policy is to outline the management, operation and use of CCTV systems (Closed Circuit Television) which may be in use at some of our sites.

Implementation: It is the responsibility of managers to ensure that staff members, people we support and visitors are aware of the presence of any CCTV system on site, as well as the accompanying *CCTV System Privacy Notice*, and that appropriate signage and management processes for the system are in place.

Compliance: This policy complies with all relevant regulations and other legislation as detailed in the *Compliance with Regulations & Legislation Statement*, and particularly the Data Protection Act 2018 and Information Commissioner's Office *Guidance for organisations using CCTV*, which provides further guidance as required.

For adult care services located in England, this policy takes into consideration guidance issued by the Quality Care Commission ('QCC'), which should be read in conjunction with this policy.

For residential childcare services located in England, this policy takes into consideration guidance issued by Ofsted, which should be read in conjunction with this policy.

For Independent schools located in England, this policy takes into consideration guidance issued by the Department of Education ('DoE'), which should be read in conjunction with this policy.

For CCTV operating in public places in England and Wales, this policy takes guidance from the Amended Surveillance Camera Code of Practice and its 12 Guiding Principles, which should be read in conjunction with this policy.

For CCTV operating in public places in Scotland, this policy takes guidance from the National Strategy for Public Space CCTV in Scotland, which should be read in conjunction with this policy.

For adult care services located in Scotland, this policy takes into consideration guidance issued by the Care Inspectorate ('CI'), which should be read in conjunction with this policy.

For health and social care services located in Northern Ireland, this policy takes into consideration guidance issued by The Regulation and Quality Improvement Authority ('RQIA'), which should be read in conjunction with this policy.

2.0 JUSTIFICATION FOR CCTV INSTALLATION

CCTV systems may be situated across some premises in order to achieve the following objectives:

- To protect people we support, staff and visitors
- To increase personal safety and reduce the fear of crime
- To protect buildings and assets
- Without prejudice, to protect the personal property of people we support, staff and visitors
- To support the police in preventing and detecting crime
- To assist in identifying, apprehending and prosecuting offenders
- To assist in managing the premises, including wildlife and animals

Data Privacy Impact Assessments: The installation of CCTV systems must only be done following completion of a *Data Privacy Impact Assessment*. This process will help to ensure that a surveillance system is justified in response to an identified risk, whether better solutions exist, what effect its use may have on the privacy of individuals, and whether in the light of this, its use is a proportionate response to the problem. Where CCTV systems have already been installed, the relevant service should ensure that a DPIA is completed and reviewed as soon as possible.

3.0 STATEMENT OF INTENT

The service will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Data Protection Act 2018.

The purposes of this system are outlined above, but predominantly cameras will be used to monitor activities within the site and its grounds to identify criminal activity occurring, anticipated, or perceived. It will be also used for securing the safety and wellbeing of the people we support, staff and property, together with visitors.

Planning and design will ensure that the system gives maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. Warning signs, as required by the ICO Code of Practice will be clearly visible on the site.

The system has been designed to deny observation on adjacent private property, and materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime, with the written authority of the police.

4.0 SYSTEM MANAGEMENT

The CCTV system will be in constant operation and managed day to day by the service locally, which will act in accordance with the principles and objectives expressed in this policy and *CCTV System Privacy Notice*. The system and the data collected will only be available to senior members of staff and selected system administrators. Any CCTV monitors will be in a locked office and secured with a strong password.

The service will check and confirm the efficiency of the system daily and, in particular, that the equipment is properly recording and that cameras are functional.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

The designated System Administrator must satisfy themselves of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists, access will be refused. Details of system access (other than the system administrator) will be recorded in the *CCTV System Log Book*, including time and date of access, purpose and details of images viewed.

All CCTV data is stored for a maximum 30 days only, at a secure locked location, after which it is automatically destroyed.

A checklist for the implementation of a CCTV system can be found at Appendix 1, together with a template *CCTV System Log Book* at Appendix 2.

5.0 SHARING CCTV IMAGES

We do not share information with any third party without the express consent of the data subject unless the Law permits us to do so. Where it is legally required, or necessary (and it complies with data protection law), we may be obligated to share CCTV data with:

- Local authorities – to meet our legal obligations to share certain information with it, such as safeguarding concerns
- Regulatory Bodies
- Central and local government
- Health authorities
- Security organisations
- Professional Legal Advisors
- Police forces, courts, tribunals

The CCTV system and images are not available to visitors except under circumstances as outlined in this policy.

6.0 IMAGE DOWNLOADING PROCEDURE

Images may be viewed by the police for the prevention and detection of crime or for other authorised applicants. In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any download media (e.g. USB stick) used to record events from the hard drive must be prepared in accordance with the following processes:

- Each download media must be identified by a unique mark.
- Before use, each download media must be cleaned of any previous recording.
- The service will register the date and time of download media insertion, including its reference, in the *CCTV System Log Book*.
- Download media required for evidential purposes must be sealed, witnessed and signed by the System Administrator, then dated and stored in a separate secure evidence store. If a download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by a senior member of staff, then dated and returned to the evidence store.
- If download media is archived, the reference must be noted.
- A record will be maintained of the release of any download media to the police or other authorised applicants.
- Viewing of images by the police must be recorded in writing.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the download media (and any images contained thereon) remains the property of the company and are to be treated in accordance with Data Protection legislation. The company also retains the right to refuse permission for the police to pass the downloaded media to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

Access by the Data Subject

The Data Protection Act provides data subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made to a senior member of staff and passed for processing to the Data Protection & Regulatory Compliance Team.

7.0 MONITORING OF CCTV MANAGEMENT & COMPLAINTS

Performance monitoring, including random operating checks on all CCTV and compliance with this policy, may be carried out as required.

Any complaints in relation to the CCTV system should be addressed to a senior member of staff.

Outcomes
FirstGroup