Document Title	**Closed Circuit Television (CCTV) Policy**
Type of document	Corporate
Brief summary of contents	• Clear guidance in the use of CCTV images • Contact details for CCTV related enquiries • Responsibilities of individuals • Information on the CCTV code of practice
SLT member responsible for policy	Executive Director of Strategic Planning & Corporate Services
Date written	26th July 2016
Date last revised	17th January 2023
This document replaces	Not applicable
Approval route/consultation	Department Head, SLT member
Head of Department (HOD) responsible for policy	Kelly Condon
Author of policy	Department Head
Contact details	DPO@rnngroup.ac.uk
Publication location	Public and portals
Date of final approval	4th March 2019
Date policy becomes live	4th March 2019
Review period	Annual
Links to external standards	ICO CCTV code of practice, The Data Protection Act 2018, The Investigatory Powers Act 2016, The Human Rights Act 1998
Related documents	• Acceptable Use Policies (AUP) • Data Protection Policy • Data Subject Access Request (DSAR) Policy • Mobile Phone Policy
Keywords	CCTV, images, IT, technology, security, recording, access, data protection
Training needs	Data Protection, CCTV operator (for authorised staff)

Closed Circuit Television (CCTV) Policy

Version 1.4

17th January 2023

Version Control Table

Date	Version No	Summary of Changes	Changes Made By
26th July 2016	1.0	Birth of policy	Ian Headley
29th November 2017	1.1	Updated contact details for SLT member, legislation update, additional guidance on the use of CCTV images	Ian Headley
30th January 2019	1.2	Legislation update, annual review	Ian Headley
4th November 2019	1.3	Annual review	Kelly Condon
17th January 2023	1.4	Job title changes, amendments to Group sites, additional guidance on the use of CCTV images 1. (1.6) and annual review.	Kelly Condon

All or part of this document can be released under the Freedom of Information Act 2000

Table of Contents

Appendices

CCTV systems are provided for site safety and the security of students, staff and any other party engaging with the RNN Group, (hereinafter referred to as the 'Group'). It will not be used to gather data for performance management purposes or in capability procedures but may be used as evidence in misconduct investigations. Signage is placed throughout the relevant Group sites informing people of its intent and directing any enquiries to the right department.

CCTV recordings are located in secure environments and are temporarily stored on disk, backups are taken, also stored in a secure location and securely destroyed in accordance with the published data retention timescales. Data may be retained for longer periods should this be needed to facilitate additional investigation or action.

The Group is classified as the Data Controller of all images captured by its CCTV systems, wherever they may be. The Group is responsible for the supply of CCTV data, images and recordings and shall adhere to the principles outlined in the Group's Data Protection Policy and related procedures, the Data Subject Access Request (DSAR) Policy and act in accordance with any other relevant legislation.

This policy applies to all Group CCTV cameras and related equipment on its various premises, it does not apply to audio-visual recordings made by Group staff for their own private use on their own personally owned equipment. However, personal use of audio-visual recordings used to harass or cause distress to others may be subject to disciplinary action in accordance with regulations and policies governing the conduct of students, colleagues or other users and may be in breach of criminal law.

This policy should also be read where body worn cameras are in operation, the same policy applies to this type of data collection and additional care should be taken by the operator of such as system to ensure recording equipment is not lost or stolen.

1. Contact

1.1 There is no public-facing direct contact telephone number for the CCTV service, all enquiries should initially be directed to the main site numbers (Worksop, including Idle Valley and National Fluid Power Centre 01909 504504, Rotherham, including UCR and Rawmarsh Road (Construction) 01709 362111 and Dearne Valley 01709 513333).

1.2 All requests for or access to possible images, or enquiries as to the locations of any cameras should be emailed to cctvenquiries@rnngroup.ac.uk unless investigations form part of a DSAR enquiry.

1.3 Group staff will not engage directly with members of the public regarding CCTV matters such as location and coverage.

1.4 Police have a right to access CCTV images but this is only permitted upon the submission of a Schedule 2 Part 1 Paragraph 2 DSAR form (or the Group equivalent, see DSAR Policy).

1.5 Except as described in section 2 below, members of staff do not have any right to view CCTV images.

1.6 Staff will not be granted access to CCTV footage of any third party for their own use (for example to identify damage to personal property).

2. Viewing of images

2.1 All requests to the Group concerning the possible existence of CCTV images for investigative purposes must come via the Police, legal representative or insurance firm, as detailed in the Investigatory Powers Act 2016 and the Data Protection Act 2018.

2.2 Unauthorised members of Group staff are NOT permitted to view any images, live or recorded without supervision from authorised staff.

2.3 Authorised Group staff are designated members of the Facilities or IT Services teams where this function is mainly based. From time to time any member of these teams may be nominated CCTV operator.

2.4 The Senior Leadership Team of the Group may instruct the nominated CCTV operator in the event of an incident occurring, including authorisation for other Group staff to view footage, where appropriate. The CCTV operator will record this instruction and the actions taken on their register of investigations.

2.5 Members of the public are NOT permitted to view any images, live or recorded, as this would be a breach of UK legislation.

2.6 The Group may levy a charge for providing footage that relates to a civil matter for example, to prove responsibility for a vehicle insurance claim (subject to receipt of the official request from the relevant insurance company).

2.7 The Group nominated CCTV operator will log all investigations and subsequent actions/outcomes and retain this detail for two years after investigations are complete.

2.8 A CCTV operator nominated by the Group will work closely with the Police and other public services, or staff, should viewing of CCTV images be necessary, this will be performed in a controlled environment.

2.9 Under no circumstances should any CCTV images be stored on any personal device e.g. mobile phone, laptop, tablet etc.

2.10 Unauthorised CCTV image access and/or sharing of images may lead to disciplinary action.

2.11 Live, recorded or still images will not be taken from the CCTV operator station without prior, approval via the Group's IT Helpdesk from the Data Protection Officer or in their absence, Executive Director of Strategic Planning & Corporate Service, Head of Estates and Facilities or Head of IT Services (or relevant deputies). The operator requesting approval should record this approval.

2.12 Live or recorded images will not be presented onto the Internet by Group staff in any form and in any circumstance, publication of CCTV images may lead to disciplinary action.

3. Retention of data

3.1 All CCTV images are destroyed after no more than 20 days and are non-recoverable, unless where an investigation is in progress or where evidence is required to be retained by law enforcement directive.

4. Monitoring

4.1 The Group cameras may be monitored 24 hours a day, 7 days a week internally or by externally contracted, qualified, CCTV operators.

4.2 Subject to the provisions herein, CCTV footage will be provided to law enforcement or other relevant agencies investigating crime.

5. Code of practice

5.1 A strict code of practice, based on the Information Commissioners Office (ICO) guidelines, governs the use of the CCTV system and relates to issues such as storage, use of the system and deletion of images and recordings. Stringent privacy regulations explicitly prohibit the commercial use of any CCTV images captured by the Group's systems.

5.2 CCTV operators authorised by the Group are expected to be aware of, and adhere to, this code of practice.

5.3 Any images supplied to the Police, legal representative or insurance firm as part of an investigation must be provided in encrypted format. If the Police request in an un-encrypted format then this should be documented by the operator performing the investigation at the time of releasing the CCTV images.

5.4 Group employees will not engage in covert surveillance of any type. If such surveillance is requested by the Police for the detection and prevention of crime, specific legal requirements will have to be satisfied, mainly contained in the Investigatory Powers Act 2016.

6. Legislation

Legislation covered within this policy:

The Investigatory Powers Act 2016 (previously known as The Regulation of Investigatory Powers Act 2000 (RIPA))
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Regulations)
The Data Protection Act 2018
The Freedom of Information Act 2000
The Human Rights Act 1998
The Privacy and Electronic Communications (EC Directive) Regulations 2003 and amendment to the Regulations 2011
The Counter-Terrorism and Security Act 2015
The Computer Misuse Act 1990
The Terrorism Act 2006
The Police and Justice Act 2006
The Crime and Disorder Act 1998
The Protection of Freedoms Act 2012
The Serious Crime Act 2015
The Copyright, Designs and Patents Act 1988
The Equality Act 2010
The Limitation Act 1980
The Malicious Communications Act 1988
The Digital Economy Act 2017
The Prevent Strategy 2011
The Care Act 2014
The Children Act 1989 and 2004
The Education Act 2011
Keeping Children Safe in Education 2022 (Education Act 2011)
The Childcare Act 2006

7. Linked Policies and Guidance

Policies and guidance linked to this policy:

Mobile Phone Policy
Data Protection Policy
Data Subject Access Request Policy
Privacy Policy