RUGBY FIRST LTD

CONTROL CENTRE

CODE OF PRACTICE FOR CCTV SCHEME

(BS7958 and the Surveillance Camera Commissioner's Code of Practice)

CONTENTS

Page: 3 of 37	**Authority: Ryan Webster**
Date: 27.5.20	

1.0 INTRODUCTIONS & DEFINITIONS

Introduction

1.1 This Code of Practice shall apply to the closed circuit television surveillance scheme known as Rugby First Ltd C.C.T.V. scheme. The scheme initially comprises of cameras located in specific external and internal locations within Rugby First area, with control, monitoring and recording facilities at a dedicated location. A problem orientated process was utilised to assess the appropriateness of CCTV in Rugby area. The cameras have therefore been sited to capture images of identifiable individuals or information relating to individuals which are relevant to the purposes for which the scheme has been established.

1.2 Ownership

The scheme is owned by Rugby First Ltd who are the Data Controller responsible for the management, administration and security of the system. Rugby First Ltd company will ensure the protection of individuals and the public by complying with the Codes of Practice.

1.3 Closed Circuit Television Mission Statement

To promote public confidence by developing a safe and secure environment for the benefit of those employed, visiting or using the facilities of the area covered by Rugby First Ltd CCTV system. Rugby First Ltd is committed to the recommendations contained in the Information Commissioners CCTV Code of Practice which can be found on the following website: www.ico.gov.uk.

1.4 Codes of Practice Mission Statement

To inspire public confidence by ensuring that all public area Closed Circuit Television (CCTV) systems which are linked to the CCTV Control and Monitoring Room are operated in a manner that will secure their consistent effectiveness and preserve the civil liberty of law abiding citizens at all times.

1.5 Definitions

1.5.1 **The CCTV control and monitoring room** shall mean the secure area of a building where CCTV is monitored and where data is retrieved, analysed and processed. It is also the location where calls may be received from 'Help Points' and from where warning can be made via public address systems, associated with the cameras.

1.5.2 **CCTV scheme** shall mean the totality of the arrangements for closed circuit television in the locality and is not limited to the technological system, staff and operational procedures.

1.5.3 **The retrieval system** means the capability, in any medium, of effectively capturing data that can be retrieved, viewed or processed.

1.5.4 **CCTV system** means the surveillance items comprising cameras and associated equipment for monitoring, transmission and controlling purposes, for use in a defined zone.

1.5.5 The distributed system means any subsystem, any part of which may be linked temporarily or permanently for remote monitoring within the CCTV system.

1.5.8 **Data** shall mean all information, including that about a person in the form of pictures, and any other associated linked or processed information.

1.5.9 **Personal Data** means data which relates to a living individual who can be identified:

a) from that data or
b) from that data and other information which is in the possession of or is likely to come into the possession of, the data controller.

1.5.10 **Sensitive personal data** is personal data which is deemed to be sensitive. The most significant of these, for the purposes of this code are information about:-

- The commission or alleged commission of any offences
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

1.5.11 **An incident** is an activity that raises cause for concern that the safety or security of an individual or property including vehicles that may be compromised or that an offence has been, is being or is about to be, committed, or that an occurrence has taken place warranting specific action by an operator.

1.5.12 **The owner** is Rugby First Ltd, the organisation with overall responsibility for the formulation and implementation of policies, purposes and control of the scheme.

1.5.13 **The manager** has the responsibility for the implementation of the policies, purposes and methods of control of a CCTV scheme, as defined by the owner of the scheme. The manager of the scheme is a designated employee of Rugby First Ltd.

1.5.14 **Data controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are about to be processed. The Data Controller for the CCTV schemes is Rugby First Ltd.

1.5.15 Operators are employees of Rugby First Ltd and are specifically designated to carry out the physical operation of controlling the CCTV system and the data generated. All operators are screened, trained and licensed to the standards required in the Private security Industry Act 2001.

1.5.16 **Recording material** means any medium that has the capacity to store data and from which data can later be recalled irrespective of time.

1.5.17 **A hard copy print** is a paper copy of a live image or images, which already exist on recorded material.

1.6 System description

1.6.1 The Closed Circuit Television system referred to in this document has been introduced into Rugby area. Whilst the schemes are owned by Rugby First and operated by their staff its implementation and/or expansion is supported by the following bodies (the partners)

1 Warwickshire Police
3 Rugby Borough Council
4 Local Management forums
5 Local Businesses

The owner, operator and all partners will work in accordance with these and the Information Commissioner's Codes. The partners will have no involvement in the operating of the system with the exception of the Police and authorised and trained personnel of Rugby First Ltd.

1.6.2 This Code of Practice shall apply to the closed circuit television surveillance systems known as Rugby First Ltd CCTV schemes.

1.6.3 The system consists of static and fully functional (pan, tilt and zoom) cameras and either a fibre optic or other transmission system which sends pictures to Rugby First Ltd control, monitoring and recording facility.

1.6.4 Images from all cameras are recorded simultaneously throughout 24 hour period 365 days each year.

1.6.5 There is also a dedicated CCTV transmission link to Police control rooms operating within the areas of CCTV coverage where live pictures and events can be monitored.

1.6.6 High quality cameras both fully functional with pan, tilt and zoom and static are in use.

1.6.7 The physical and intellectual rights in relation to any and all material recorded within Rugby First Ltd Control and Monitoring facility shall at all times remain in the ownership of Rugby First

2.0 CHANGES TO THE CODE OF PRACTICE

2.1 Consultation

Any major changes to this Code of Practice will take place only after consultation with the relevant management group and upon agreement of all organisations with a participatory role in the operation of the system.

2.1.1 Major changes to this code are defined as changes which affect its fundamental principles and shall be deemed to include:

- additions and omissions of cameras to the system (These can only be undertaken with the express agreement of the Home Office – at least for the first 5 years of the scheme)
- matters which have privacy implications
- additions to permitted uses criteria e.g. purposes of the scheme
- changes in the right of access to personal data, except statutory requirements
- significant legal implications.

2.1.2 Minor changes to this Code of Practice are defined as operational and procedural matters which do not affect the fundamental principles and purposes; these include:

- additions and omissions of contractors
- additional clarifications, explanations and corrections to the existing code
- additions to the code of practice in order to conform to the requirements of any statutory Acts and changes in criminal legislation

A minor change may be agreed between the manager and the owner of the system.

The Code of Practice will be subject to annual review which will include compliance with the relevant legislation and Standards.

2.2 Supplementary Documentation

The Code of Practice will be supplemented by the following documents:

- CCTV Operations Procedural Manual
- Manufacturers Equipment manual

Each document contains instructions and guidance to ensure that the objectives and principles set out in this Code of Practice are achieved. These documents will be restricted to the partners and staff members only.

3.0 OBJECTIVES OF THE CCTV SCHEME & CODE OF PRACTICE

3.1 Purpose of and Compliance with the Code of Practice

3.1.1 This Code of Practice is to detail the management, administration and operation of the closed circuit television (CCTV) system in Rugby area and the associated Control and Monitoring Facility.

3.1.2 The Code of Practice has a dual purpose, in that it will assist owners, management and operators to understand their legal and moral obligations whilst reassuring the public about the safeguards contained within it.

3.1.3 The owners, CCTV Operators and users of the CCTV systems and associated safety and security equipment connected to the Control, Monitoring and Recording facility shall be required to give a formal undertaking that they will comply with this Code of Practice and act in good faith with regard to the basic principles contained within it.

3.1.4 The owners, CCTV Operators, users and any visitors to the Control, monitoring and recording facility will be required to sign a formal confidentiality declaration that they will treat any viewed and/or written material as being strictly confidential and that they undertake not to divulge it to any other person.

3.2 Objectives of the scheme

3.2.1 The following objectives have been established for Rugby First Ltd CCTV and associated systems:

(a) reducing the fear of crime

(b) deterring and preventing crime

(c) assisting in the maintenance of public order and reducing offences involving vandalism and nuisance

(d) providing high quality evidence which may assist in the detection of crime and the apprehension and prosecution of offenders

(e) protecting property

(f) providing assistance with civil claims

(g) providing assistance with issues relating to public safety and health

(h) providing assistance and reassurance to the public in emergency situations

4.0 FUNDAMENTAL PRINCIPLES & POLICIES

4.1 Rights of Privacy

4.1.2 Rugby First Ltd and partners support the individual's right to privacy and will insist that all agencies involved in the provision and use of Public surveillance CCTV systems connected to the control, monitoring and recording facility accept this fundamental principle as being paramount.

4.2 Principles of management of the scheme

4.2.1 Prior to the installation of cameras an 'Impact Assessment' to determine whether CCTV is justified and how it will be operated will be undertaken in compliance with the Surveillance Camera Commissioner's CCTV Code of Practice.

4.2.2 The cameras have been sited to capture images which are relevant to the specified purposes for which the scheme has been established.

4.2.3 Cameras will be sited to ensure that they can produce images of the right quality, taking into account technical and environmental issues.

4.2.4 To accomplish the above an 'Operational Requirement' will be completed at the time of the 'Impact Assessment' for each proposed camera to dictate the quality of images required. This is a recommendation of the information Commissioner.

4.2.5 Help Points are to be used in conjunction with the cameras. The audio communications incorporated in the help points are initiated by those requiring assistance and cannot be used to record conversations between members of the public

4.2.6 If wireless transmission systems are used to control CCTV equipment, sufficient safeguards will be in place to protect them from being intercepted.

4.2.7 The scheme will be operated fairly, within the applicable law and only for the purposes for which it is established or which are subsequently agreed in accordance with the Code of Practice.

4.2.8 Operators are aware of the purpose(s) for which the scheme has been established and that the CCTV equipment is only used to achieve the identified purposes.

4.2.9 The scheme will be operated with due regard for the privacy of the individual.

4.2.10 Before cameras are placed in residential areas the residents in that area will be consulted concerning the proposed system. The results of the consultation will be taken into account.

4.2.11 The public interest in the operation of the scheme will be recognised by ensuring the security and integrity of operational procedures.

4.2.12 The system will only be operated by trained and authorised personnel.

4.3 Policy of the Scheme and Signage

4.3.1 Signage

The scheme aims to provide surveillance of the public areas within designated areas of Rugby in order to fulfill the stated purposes of the scheme. The area protected by CCTV will be indicated by the presence of signs. The signs will be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment. The signs will state the organisation responsible for the scheme, the purposes of the scheme and a contact telephone number. Data will not be held for longer than necessary and disposal of information will be regulated.

4.3.2 Help Points

Help Points are installed in strategic locations within Rugby Town Centre. The Help Points are two way audio feeds covered by CCTV cameras and can be activated by a person requiring assistance they should be used predominantly in emergency situations. The Help points will be monitored by the CCTV system and conversations with the CCTV control centre will be recorded. Procedures adopted for the use of the Help points will adhere to the required legislation. Where audio recording is undertaken the signage mentioned in 4.3.1 will make this clear.

4.4 Point of contact

Should the public wish to make contact with the owners of the scheme they may write to:

The BID Manager
Rugby First Ltd
Bloxam Court
Corporation Street
Rugby
CV21 2DU

The contact point will be available to members of the public during office hours. Enquirers will be provided with the relevant documentation.

4.5 Release of information to the public

Information will be released to third parties, itemised in Section 8 who can show legitimate reasons for access. They will be required to request any information with reasons in writing and identify themselves.
Information will only be released if the data captures identifiable individuals or information relating to individuals and the reasons are deemed acceptable, the request and release of information complies with current legislation and on condition that the information is not used for any other purpose than that specified.

Individuals may request to view information concerning themselves held on record in accordance with the Data Protection Act 2018 and the General Data Protection Regulation. The procedure is outlined in Section 8.9 of this Code of Practice.

4.6 Release of information to statutory prosecuting bodies

The policy is to assist statutory prosecuting bodies such as the Police, and statutory authorities with powers to prosecute and facilitate the legitimate use of the information derived from the scheme. Statutory bodies may have access to information permitted for disclosure on application to the owner of the scheme or the manager, provided the reasons and statement of purpose, accord with the objectives of the scheme and conditions outlined in section 8.0. The information will be treated as evidential exhibits.

4.7 Annual policy review

There will be an annual policy review covering the following aspects:

a) whether the purpose and objectives statements remain valid
b) change in extent of the scheme
c) contracts with suppliers
d) a review of the data protection or legal requirements
e) maintenance schedule and performance test of the system
f) scheme evaluation findings
g) complaints process and evaluation

5.0 DATA PROTECTION ACT AND OTHER LEGISLATION

5.1.1 The scheme is registered with the Data Protection Commissioner, Registration Number: Z8185981. The scheme will be managed in accordance with the principles of the Data Protection Act 2018 and the Articles of the General Data Protection Regulation.

5.2 Human Rights Act 1998

The system will be operated by or on behalf of a public authority, the authority has considered the wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life).

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Therefore, to comply with Article 8 (1), and Article 8 (2) Rugby First will always consider the following:

Proportionality - Article 4.2.1, 4.2.2, 4.2.3 and 4.2.6 of the code of practice
Legality - Article 4.2.7 and 4.2.8 of the code of practice
Accountability - Article 4.2.10 and 4.2.11 of the code of practice
Necessity/Compulsion - Article 4.2.3 of the code of practice

Any infringement by a public authority of another's rights must be justified.

If this is not the case then it will not be appropriate to use CCTV.

5.3 Criminal Procedures and Investigations Act 1996

The Criminal Procedures and Investigations Act 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the prosecution of its own case (known as unused material) but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by the Data Protection Act 2018 and the General Data Protection Regulation (known as subject access).

5.4 Freedom of Information Act 2000

If a request for images is received via a FOIA application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under The Data Protection Act and the Articles of the General Data Protection Regulation.

Any other requests not involving identification of individuals can be disclosed but only if it does not breach the data protection principles.

5.5 Regulation of Investigatory Powers Act 2000

Introduction
The Regulation of Investigatory Powers Act 2000 came into force on 2nd October 2000. It places a requirement on public authorities listed in Schedule 1: Part 1 of the act to authorise certain types of covert surveillance during planned investigations.

Background
General observation forms part of the duties of many law enforcement officers and other public bodies. Police officers will be on patrol at football grounds and other venues monitoring the crowd to maintain public safety and prevent disorder. Officers may also target a crime "hot spot" in order to identify and arrest offenders committing crime at that location. Trading standards or HM Customs & Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve **systematic surveillance of an individual**. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2000 Act.

Neither do the provisions of the Act cover the normal, everyday use of **overt** CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. However, it had not been envisaged how much the Act would impact on specific, targeted use of public/private CCTV systems by 'relevant Public Authorities' covered in Schedule 1: Part1 of the Act, when used during their planned investigations.

The consequences of not obtaining an authorisation under this Part may be, where there is an interference by a public authority with Article 8 rights (invasion of privacy), and there is no other source of authority, that the action is unlawful by virtue of section 6 of the Human Rights Act 1998 (Right to fair trial) and the evidence obtained could be excluded in court under Section 78 Police & Criminal Evidence Act 1984.

The Act is divided into five parts. Part II is the relevant part of the act for CCTV. It creates a system of authorisations for various types of covert surveillance. The types of activity covered are "intrusive surveillance" and "directed surveillance". Both types of surveillance if part of a pre-planned operation will require authorisation from specified persons named in the Act. In addition, the reasons for such surveillance must be clearly indicated and fall within the criteria outlined by this legislation. A procedure is in place for regular reviews to be undertaken into authorisation.

Rugby First Ltd scheme will observe the criteria laid out in the legislative requirements.

Further information is available from the Home Office website:-

www.homeoffice.gov.uk/ripa/ripact.htm

5.6 Surveillance Camera Code of Practice

The Code of Practice was a requirement of the Protection of Freedoms Act 2012 and sets out guidelines for the CCTV system to ensure their use is open and proportionate and that they are able to capture quality images that give police a better chance to catch criminals and cut crime.

The code has been built upon 12 guiding principles, which provide a framework of good practice that includes existing legal obligations. Those existing obligations include the processing of personal data under the Data Protection Act 2018 and the General Data Protection Regulation, a public authority's duty to adhere to the Human Rights Act 1998 and safeguards under the Regulation of Investigatory Powers Act 2000 associated with the use of directed and covert surveillance by a public authority. The use of a surveillance camera system must:

1. Always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
2. Take into account its effect on individuals and their privacy
3. Have as much transparency as possible, including a published contact point for access to information and complaints
4. Have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
5. Have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
6. Have no more images and information stored than that which is strictly required
7. Restrict access to retained images and information with clear rules on who can gain access

8. Consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
9. Be subject to appropriate security measures to safeguard against unauthorised access and use
10. Have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with
11. Be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim
12. Be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.

Whilst the above principles are voluntary, Local Authorities must have regard to them and Rugby First Limited will work to achieve continued compliance with the requirements.

5.7 Crime & Courts Act 2013

The Crime and Courts Act became law on 1st October 2013 and replaced the Serious Organised Crime and Police Act 2005. CCTV Control Rooms, RVRC's and the like are under Section 7 of the Crime & Courts Act 2013 required by law to share information (CCTV images) to the National Crime Agency (NCA). If a request is received from the NCA then Rugby First CCTV Control Room MUST comply with the request and provide the data.

Section 7, Subsection (3) provides information obtained by the NCA in connection with the exercise of any NCA function may be used by the NCA in connection with the exercise of any other NCA function. For example, information obtained in the course of gathering criminal intelligence may be used in connection with NCA's crime reduction function.

Section 7, Subsection (4) provides that the NCA may disclose information in connection with the exercise of any NCA function if the disclosure is for any "permitted purpose" as defined within Section 16(1) of the Act. This would apply in situations where, for example, the NCA has received information on suspected criminal activity (such as a 'Suspicious Activity Report' – which help banks and financial institutions protect themselves and their reputation from criminals and help law enforcement to track down and arrest them) and has decided to share this information with an organisation or person outside the NCA (such as a financial institution) for the purpose of preventing or detecting crime.

6.0 ACCOUNTABILITY

6.1 Rugby First and the Partners support the principle that the community at large should be satisfied that the Public surveillance CCTV systems are being used, managed and controlled in a responsible and accountable manner and that in order to meet this objective there will be independent assessment and scrutiny. It is the responsibility of all parties to maintain a continuous review of it's integrity, security, procedural efficiency, methods of operation and retention and release of data.

6.2 Hierarchy of Responsibilities

6.2.1 **The Owner**

The owner shall be responsible for policy, effective management and public relations of the scheme. They shall produce a written policy and be responsible for its implementation. This shall be carried out in consultation with users of the scheme and provide for the release of information relating to the operation of the system. The owner is responsible for dealing with complaints and ensuring a fair system of staff selection and recruitment is adopted for staff employed in the control and monitoring environment. The role of owner also includes all statutory responsibilities including the role of "data controller" as prescribed by the Data Protection Act 2018. The Single Point of Contact for Rugby First is the BID Manager and the Single Responsible Officer is the Operations Director.

6.2.2 **The Manager**

The manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with. These should be reported back to the owner of the scheme. To facilitate this, regular minuted meetings will be held with the Supervisor to go through the points listed below:-

<u>The manager is the person who has direct control of the scheme and as such he/she will have authority for the following</u>

- Staff management
- Observance of the policy and procedural practices
- Release of data to third parties who have legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new and destruction of old data
- Liaison with police and other agencies
- Maintenance of the quality of recording and monitoring equipment

The manager should retain responsibility for the implementation of procedures to ensure that the system operates according to the purposes for which it was installed and in accordance with the objectives identified for the system.

The manager shall also ensure that on a day-to-day basis all equipment is working correctly and that the operators of the scheme comply with the Code of Practice and Procedural Manual. Dealing with breaches of the codes and disciplinary measures shall lie with the manager.

6.2.3 **The Supervisor**

The supervisor has a responsibility to ensure that at all times the system is operated in accordance with the policy and all procedural instructions relating to the system, and for bringing to the immediate attention of the manager any matter affecting the operation of the system, including any breach or suspected breach of the policy, procedural instructions, security of data or confidentially.

In the Manager's absence the Supervisor will have responsibility for:

- Release of data to third parties who have legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new Media
- Liaison with police and other agencies

The supervisor should ensure that at all times operators carry out their duties in an efficient and responsible manner, in accordance with the objectives of the scheme. This will include regular checks and audit trails to ensure that the documentation systems in place are working effectively. These systems include:

- The media log
- The media register
- The operators log
- The incident log
- Witness statements
- Faults and maintenance log
- The security of data
- Audit logs
- Authorisation of visitors – to be checked & counter signed by the Supervisor

The supervisor will ensure operators comply with Health and Safety Regulations.

6.2.4 The Operators

The operators will be responsible for complying with the code of practice and procedural manual. They have a responsibility to respect the privacy of the individual, understand and comply with the objectives of the scheme. They are required to be proficient in the control and the use of the CCTV camera equipment, recording and playback facilities, media erasure, and maintenance of all logs. The information recorded must be accurate, adequate and relevant to the purpose of the scheme. They should bring to the attention of the supervisor immediately any equipment defect that may occur.

In the Managers/Supervisors absence the Operator will have responsibility for:

- Release of data to third parties who have legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new Media
- Liaison with police and other agencies

6.2.5 Contractor's Responsibilities

There is a contractor responsible for the Maintenance of CCTV equipment. The response provided by contractors is subject of a written contract and records of responses are maintained.

6.3 Accountability

The manager/supervisor shall be accountable to the owner of the scheme and will provide periodic progress reports on the scheme. The manager/supervisor will resolve technical and operational matters.

Failure of the operators to comply with the procedures and code of practice should be dealt with by the manager/supervisor. Person(s) misusing the system will be subject to disciplinary or legal proceedings in accordance with the employer's policy.

6.4 Annual Assessment

An annual assessment of the scheme will be undertaken by an independent consultancy appointed by the owner to evaluate the effectiveness of the system. This will include annual reviews of the scheme's operation, performance and working practices and, where appropriate make recommendations for improvements. The results will be assessed against the stated purposes of the scheme. If the scheme is not achieving its purpose modification and other options will be considered. The results of the assessment will be made available through Rugby First Ltd offices.

It is a recommendation of the Information Commissioner that the CCTV system should be reviewed annually to determine whether CCTV continues to be justified.

6.5 Audit

Regular independent random audits will check the operation of the scheme and the compliance with the code of practice. It will consider the following:

- The level of attainment of objectives and procedures
- Random audits of the data log and release of information
- The review policy
- Standard costs for the release of viewing of material
- The complaints process
- Compliance with procedures

6.6 Complaints

A member of the public wishing to make a complaint about the system may do so through Rugby First Ltd's complaint procedure. Copies of the complaints process are available by writing to:

The BID Manager
Rugby First Ltd
Bloxam Court
Corporation Street
Rugby
CV21 2DU

A complaints process has been documented. A record of the number of complaints or enquiries received will be maintained together with an outline of the action taken.

When a complaint is received a written acknowledgement will be sent within three working days. A copy of the completed complaint form will also be sent so the complainant can check that the details are correct.

An investigation will follow and a written answer will be sent to the complainant within fifteen working days stating that:-

- the investigation is complete giving details of any proposed action, or, the investigation has not been completed giving the reason why and a date when a full reply can be expected.

Should a complainant not be satisfied there is an appeals procedure and this is detailed in the full complaints process.

A report on the numbers of complaints will be collated by the systems manager or designated member of staff in order to assess public reaction to, and opinion of, the use of the system. The annual report will contain details of the numbers of complaints received, the time taken to acknowledge and respond to complaints, the method of receiving and handling complaints and the degree of satisfaction in handling complaints.

6.7 Personnel

6.7.1 Security screening

All personnel employed to control/operate or manage the scheme will be security screened in accordance with British Standard 7858: *Code of practice for screening of personnel in a security environment.*

6.7.2 Training

All operators are or will be trained to the criteria required by the private Security Industry Act 2001 and licensed by the Security Industry Authority for Public Space Surveillance systems.

All persons employed to act as operators of the system are trained to the highest available industry standard. Training has been completed by suitably qualified persons and has included:

Terms of employment
The use of all appropriate equipment
The operation of the systems in place
The management of recorded material including requirements for handling and storage of material needed for evidential purposes.
All relevant legal issues including Data Protection and Human Rights
Progression to nationally recognized qualifications
Recognise and understanding privacy and disclosure issues
The disciplinary policy

6.7.3 Contractor's

There are special condition's imposed upon contractor's carrying out works on the system. These are detailed in the Procedural Manual. It should be noted that wherever possible contractors should not have sight of any recorded data.

7.0 CONTROL ROOM MANAGEMENT AND OPERATION

7.1 Access to Control Room

7.1.1 Access to the monitoring area will be strictly controlled. Security of the Control Room shall be maintained at all times.

7.1.2 Only those persons with a legitimate purpose will be permitted access to the control and monitoring Room.

7.1.3 The Manager or in his/her absence the Deputy, is authorised to determine who has access to the monitoring area. This will normally be:

(i) Operating staff
(ii) The manager/Supervisor
(iii) Police officers requiring to view images or collecting/returning media being considered for intelligence or evidential purposes. These visits will take place by prior appointment.
(iv) Engineers and cleaning staff (These people will receive supervision throughout their visit)
(v) Independent Inspectors appointed under this Code of Practice may visit the control room without prior appointment.
(vi) Organised visits by authorised persons in controlled circumstances

All visitors to the monitoring area, including Police Officers, will be required to sign a visitor's log and a declaration of confidentiality.

7.2 Response to an incident

7.2.1 The Procedural Manual details:

What action should be taken
Who should respond
The time scale for response
The times at which the observation should take place

7.2.2 A record of all incidents will be maintained in the incident log. Information will include anything of note that may be useful for investigative or evidential purposes.

7.3 Who makes the response and the time scale

Incidents of a criminal nature will be reported to the Warwickshire Police. The response will be made by the Police Service in accordance with their policies.

7.4 Observation and recording of incidents

Recording will be throughout the 24 hour period in both real time and time lapse later mode. Wherever possible the system will be monitored 24 hours a day. In the event of an incident being identified there will be particular concentration on the scene and the operator will activate real time recording.

7.5 A successful response

7.5.1 The criteria for measuring a successful response are:

A good observational record of the incident
A short time scale for response to the incident
Identification of a suspect
The prevention or minimisation of injury or damage
Reduction of crime and disorder
Improving public safety
Restoration of tranquillity

7.6 Operation of the System by the Police

a) There is a monitoring facility installed at specific Police Stations. Under certain circumstances the Police may make a request to remotely observe a number of cameras to which this Code of Practice applies. Following agreement by the control room supervisor at the time, the Police communications supervisor will provide sufficient information to the operator of the genuine need for control.

b) In the event of the police requesting use of the equipment from within the CCTV control room to monitor situations, such a request will only be permitted on the request of a Superintendent or his designated deputy and only with the permission of the BID Manager or his designated deputy. The request should be in writing, however, in emergencies this can be a verbal request which should then be followed by the written request as soon as practicable. the monitoring room will continue to be staffed and equipment operated by, only those personnel who are authorised to do so and who fall within the terms of this Code.

c) In very extreme circumstances such as a major incident a request may be made for the Police to take total control of the system in its entirety, including the staffing of the monitoring room and personal control of all associated equipment; to the exclusion of all representatives of the system owners. A request for total exclusive control must be made in writing by a Police Officer not below the rank of Superintendent (or designated deputy).

Once the police undertake any of the above the become responsible under the Data Protection Act 2018. A radio/telephone link through to the police station is available to effectively relay information on incidents that arise.

8.0 PRIVACY AND DISCLOSURES ISSUES

8.1 Privacy

Cameras should not be used to infringe the individual's rights of privacy. The cameras generally are sited where they will not be capable of viewing any residential properties. If it is found there is a possibility that cameras would intrude in private areas, privacy zones would be programmed into the cameras where possible and/or CCTV operators trained to recognise privacy issues.

The public address system should be moderated in volume so as not to intrude into the space of neighbouring properties.

8.2 Disclosure Policy

8.2.1 The following principles must be adhered to:

a) All employees will be aware of the restrictions set out in this Code of Practice in relation to access to, and disclosure of, recorded images.
b) Images not required for the purposes of the scheme will not be retained longer than necessary. However, on occasions it may be necessary to retain images for longer period, where a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation.
c) The Data controller will only disclose to third parties who intend processing the data for purposes which are deemed compatible with the objectives of the CCTV scheme.
d) Monitors displaying images from areas in which individuals would have an expectation of privacy will not be viewed by anyone other than authorised employees of the user of the equipment.
e) Recorded material will only be used for the purposes defined in the objectives and policy.
f) Access to recorded material will be in accordance with policy and procedures.
g) Information will not be disclosed for commercial purposes and entertainment purposes.
h) All access to the medium on which the images are recorded will be documented.
i) Access to recorded images will be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment.
j) Viewing of the recorded images should take place in a restricted area.

8.2.2 Before data is viewed by a third party the manager should be satisfied that data is:

a) The subject of a complaint or dispute that is unanswered
b) The original data and the audit trail is maintained throughout
c) Not part of a current criminal investigation by the Police, or likely to be so
d) Not part of a civil proceeding or likely to be so

e) Not removed or copied without proper authority
f) The image obtained is aimed at identifying individuals or information relating to an individual.

8.3 Access to recorded images

Access to recorded images will be restricted to the manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the disclosure policy.

8.4 Viewing recorded images

Where possible, the viewing of recorded images should take place in a restricted area. Other employees should not be allowed to have access to that area when viewing is taking place.

8.5 Operators

All operators are trained in their responsibilities in relation to access to privacy and disclosure issues, in addition to being licensed as previously mentioned.

8.6 Removal of medium for Viewing

The removal of medium on which images are recorded, for viewing purposes, will be documented in accordance with the Data Protection Act and the procedural manual.

8.7 Access to data by third parties

8.7.1 Access to images by third parties will only be allowed in limited and prescribed circumstances. In the case of Rugby First Ltd CCTV scheme, disclosure will be limited to the following:-

a) law enforcement agencies where the images recorded would assist in a specific criminal enquiry
b) prosecution agencies
c) legal representatives
d) the media, where it is assessed by the Police that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that assessment the wishes of the victim of an incident should be taken into account.
e) The people whose images have been recorded and retained (Data Subject) unless disclosure to an individual would prejudice the criminal enquiries or criminal proceedings.

8.7.2 All requests for access or for disclosure will be recorded. If access or disclosure is denied, the reason should be documented.

8.7.3 If access to or disclosure of the images is allowed, details will be documented.

8.7.4 Recorded images should not in normal circumstances be made more widely available, for example, they should not be routinely made available to the media or placed on the internet.

8.7.5 If it is intended that the images will be made more widely available, that decision should be made by the manager or designated member of staff and the reason documented.

8.7.6 The owner should not unduly obstruct a bone fide third party investigation to verify the existence of relevant data.

8.7.6 The owner should not destroy data that is relevant to previous or pending search request which may become the subject of a subpoena.

8.7.7 The owner should decide which other agencies, if any, should have access to data and it should be viewed live or recorded but a copy should never be made or released.

8.8 Disclosure in the public interest

Requests to view personal data that do not fall within the above categories but that may be in the public interest should be considered. Examples may include public health issues, community safety or circumstances leading to the prevention or detection of crime. Material released to a third party for the purposes of crime prevention or detection, should be governed by prior written agreement with the Chief Constable.

Material may be used for bona fide training such as Police or staff training.

8.9 Data subject access disclosure

8.9.1 All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and be aware of individual's rights under this section of the Code of Practice.

8.9.2 Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This must be provided within 40 calendar days of receiving a request.

8.9.3 Data subjects requesting access will be provided with a standard subject access request form (Appendix 'A') and accompanied leaflet (Appendix 'B') describing the types of images recorded and retained and the purposes for recording and retention.

8.9.4 Subject access rights are governed by the Data Protection Act 2018 and include the following provisions:

a) a person gives sufficient and accurate information about a date, time and place
b) information required as to the identification of the person making the request.
c) the Data Controller only shows information relevant to the search

8.9.5 If a copy is requested, it will be necessary to ascertain whether the images obtained are aimed at learning about the Data Subjects activities. If this is not the case and there has been no captured images of identifiable individuals or information relating to individuals then this may not fall within the Data Protection Act 2018 and access may be denied. Any refusal should be documented

8.9.6 If on the other hand images have been obtained and CCTV used to focus on the activities of particular people either by directing cameras at an individual's activities, looking out for particular individuals or examining recorded CCTV images to find things out about the people in them such as identifying a criminal or a witness or assessing how an employee is performing. These activities will still be covered by the DPA and reference should be made to Section 8.2.2 of these Codes of Practice prior to the release of such data.

8.9.7 If images of third parties are also shown with the images of the person who has made the access request, consideration will be given as to whether there is a need to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured. In many cases, images can be disclosed as there will not be such intrusion.

8.9.8 The subject access request will be dealt with promptly and in any case within 30 days of receipt of the request or within 30 days of receiving all the information required.

8.9.9 All subject access requests should be dealt with by the manager or designated member of staff.

8.9.10 A search request should provide sufficient information to locate the data requested (e.g. within 30 minutes for a given date and place). If insufficient information is provided a data controller may refuse a request until sufficient information is provided.

8.9.11 Under certain circumstances (Data Protection Act 2018) the manager or designated member of staff can decide that a subject access request is not to be complied with. In such cases the refusal will be documented.

Page: 28 of 37	**Authority: Ryan Webster**
Date: 27.5.20	

8.10 Provision of data to the individual

The owner/manager having verified the validity of a request should provide requested material to the individual. Where a decision has been made that third parties should not be identifiable, then arrangements will be made to disguise or blur the images in question. It may be necessary to contract this work out to another organisation. Where this occurs there will be a written contract with the processor which specifies exactly how the information is to be used and the provision of explicit security guarantees. The procedure outlined in Rugby First Procedural Manual will be followed.

If the individual agrees it may be possible to provide subject access by viewing only. If this is the case:

Viewing should take place in a controlled environment
Material not relevant to the request should be masked or edited out

8.11 Other rights

8.11.1 All staff involved in operating the equipment must be able to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage to that individual.

8.11.2 In relation to a request to prevent processing likely to cause substantial and unwarranted damage, the manager or designated member of staff's response should indicate whether he or she will comply with the request or not.

8.11.3 The member or designated member of staff must provide a written response to the individual within 21 days of receiving the request setting out their decision on the request.

8.11.4 If the manager or designated member of staff decide that the request will not be complied with, they must set out their reasons in the response to the individual.

8.11.5 A copy of the request and response will be retained.

8.12 Media Disclosure

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet. Images can be released to the media for identification purposes; this will not generally be done by anyone other than a law enforcement agency.

9.0 RECORDED MATERIAL MANAGEMENT

9.1 Retention of Images

Images, which are not required for the purpose(s) for which the equipment is being used will not be retained for longer than is necessary. As mentioned previously, on occasions images may need to be retained for longer periods as a requirement of an investigation into crime. While images are retained access to and security of the images will be controlled in accordance with the requirements of the Data Protection Act.

9.1.1 Recorded material should be of high quality. In order for recorded material to be admissible in evidence total integrity and continuity must be maintained at all times.

9.1.2 Security measures will be taken to prevent unauthorised access to, alteration, disclosure, destruction, accidental loss or destruction of recorded material.

9.1.3 Recorded material will not be released to organisations outside the ownership of the system other than for training purposes or under the guidelines referred to previously.

9.1.4 Images retained for evidential purposes will be retained in a secure place where access is controlled.

9.2 Quality and Maintenance

In order to ensure that clear images are recorded at all times the equipment for making recordings and any associated security equipment including, help points and public address systems will be maintained in good working order with regular servicing in accordance with the manufacturer's instructions. In the event of a malfunction the equipment will be repaired within specific time scales which will be scheduled within the maintenance agreement. All documentation relating to the equipment and its servicing and malfunction is retained in the control room and will be available for inspection and audit.

9.3 Digital Recordings

In a digital CCTV system, where possible, the register should show the life of the recorded media at all stages whilst in the owner's possession. Such a register may also show itself to be useful in enabling evaluation of the CCTV scheme.

The register should include the following:

1) unique equipment reference number(s);
2) time/date/person removing medium from secure storage for use;
3) time/date/person returning medium to secure storage after use;

4) remarks column to cover additional points (e.g., erase/destroy/handed over to law enforcement agencies/removed from recording machine);
5) time and date of delivery to the law enforcement agencies, identifying the law enforcement agency officer concerned;
6) in the event of a non-automated system of erasure of data, the time/date/person responsible for erasure and/or destruction
7) details of all reviews of images, including persons present and results.

9.4 Making Recordings

Details of the recording procedures are given in the Procedural Manual.

Recording mediums containing original incidents should not be replayed, unless absolutely essential to avoid any accident, damage or erasure. If recorded images need to be reviewed the reasons and details of those present will be logged and the medium returned to secure storage, if appropriate.

9.5 Video Prints

Video prints will only be made when absolutely necessary. Video Prints requested by police must be on written authority of an officer of the rank of Inspector or above. All video prints will remain the property of the scheme owner and those not handed to the police will be retained in a secure cabinet until destruction is authorised. The taking of video prints will be recorded in a register to be retained in the control room.

10.0 DOCUMENTATION

10.1 Log books must be sequential in order that pages or entries cannot be removed and full and accurate records kept.

10.2 Logs

An accurate log of operator working times will be maintained. Each operator will maintain a log of any event or occurrence including:

a) help point activity
b) public address use

10.3 Administrative documents

The following shall be maintained:

video/digital tracking register
occurrence/incident Book
visitors register
maintenance of equipment, whether routine or breakdown
staff signing on and off duty
video print log
list of installed equipment

Page: 32 of 37	**Authority: Ryan Webster**
Date: 27.5.20	

Appendix 'A'

Data Protection Act 2018 CCTV Subject Access and Third Party Request

How to Apply For Access To Information Held On the CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of the information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or data does not fall within the Data Protection Act 2018 or if you agree otherwise. Rugby First Ltd will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, Rugby First Ltd is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

Rugby First Ltd CCTV System Rights

Rugby First Ltd may deny access to information where the Act allows or does not apply. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders
- Where the Data protection Act 2018 does not apply (Where not used to capture identifiable individuals or information relating to individuals)

And giving you the information may be likely to prejudice any of these purposes.

An application form to request footage is available by contacting:

The BID Manager
Rugby First Limited
PO BOX 4481
Rugby
CV21 9DU

Page: 33 of 37	**Authority: Ryan Webster**
Date: 27.5.20	

Things to note about CCTV Subject Access Requests:

Images are held for a maximum of **28 days** from time of recording, after which they are automatically overwritten. If the relevant images are held and there are no issues affecting disclosure (see below) it will be provided either as still images or as a written description of the footage.

PLEASE NOTE THIRD PARTY DETAILS, INCLUDING VEHICLE REGISTRATION NUMBERS CANNOT BE DISCLOSED.

The request will not be successful if, for example, you do not provide enough detail about the incident, your timeframe is too broad or it is not a Rugby First camera.

Page: 34 of 37	**Authority: Ryan Webster**
Date: 27.5.20	

Appendix 'B'

CCTV SCHEME LEAFLET

The Data Protection Act 2018

CCTV IN OPERATION

This brochure contains advice and information regarding data recorded by the CCTV system and gaining access to that data.

The BID Manager
Rugby First Ltd
Bloxam Court
Corporation Street
Rugby
Warwickshire
WV21 2DU

Page: 35 of 37	**Authority: Ryan Webster**
Date: 27.5.20	

Appendix 'C'

THE PURPOSES FOR WHICH IMAGES ARE RECORDED

Full details of the principles and criteria under which this system operates may be found in the CCTV code of Practice. The aims and key objectives of the system are:

The following purposes have been established for the Rugby First Ltd CCTV and associated systems:

(a) reducing the fear of crime

(b) deterring and preventing crime

(c) assisting in the maintenance of public order and reducing offences involving vandalism and nuisance

(d) encouraging the use of the facilities offered by Rugby First Ltd

(e) providing high quality evidence which may assist in the detection of crime and the apprehension and prosecution of offenders

(f) protecting property

(g) providing assistance with civil claims

(i) providing assistance with issues relating to public safety and health

(j) providing assistance and reassurance to the public in emergency situations

RUGBY FIRST LTD

CCTV SCHEME

CODE OF PRACTICE

Copies of the Code of Practice are available free of charge on application to the CCTV System Manager.

RECORDED IMAGES

The CCTV system operates 24 hours per day, every day of the year. All cameras are continuously recorded in a multiplex time lapse mode. Additional recordings may be made of individual camera pictures in either 12 hour or 3 hour (real time) mode.

All recordings are retained for a minimum of 28 days. If no legitimate requests for retention of the recording has been made it is then erased. All requests for retention of recordings are considered against the provisions of the Data Protection Act, Human Rights Act and the Code of Practice.

The storage, processing and use of the recorded data obtained by the CCTV system is guided by the following general principles.

Recorded data will only be used for the purposes defined in the Code of Practice and in accordance with the provisions of the Data Protection Act and Human Rights Act.

Access to recorded data shall only take place in the circumstances defined in the Code of Practice and the provisions of the relevant legislation.

Recorded data will not be sold or used for commercial purposes or the provision of entertainment.

The showing of recorded data to the public will only be permitted in accordance with the law in relation to the investigation, prosecution or prevention of crime.

Data released shall remain the property of Rugby First Ltd.

Page: 37 of 37	**Authority: Ryan Webster**
Date: 27.5.20	

DISCLOSURE POLICY

Disclosure of data obtained by the CCTV System will only be committed in accordance with the relevant legislation and the criteria contained within the Code of Practice.

In every case a documented procedure, clearly showing the reasons for the request will be completed

The code lists third parties from who requests to view data will be regarded as 'primary requests' and sets out circumstances in which such applications may be made.

Third parties include:

The Police; Fire Service; H.M. Customs & Excise; Rugby First Ltd (Specific Officers); Other statutory prosecuting bodies (e.g. Trading Standards, Ministry of Defence Police; British Transport Police; etc); solicitors; plaintiffs/defendants and persons exercising their rights of subject access under the Data Protection Act 2018.

SUBJECT ACCESS

If you wish to exercise your rights of subject access as provided for in section 7 of the Data Protection Act 2018 you will be required to make the request in writing on a standard subject access request form.

All requests for subject access will be dealt with by the CCTV Manager or a nominated deputy. A written response to the request will be provided within 30 days of receipt, either setting out the steps intended to take to comply with the request or setting out the reason for refusing the request.

The Data Protection Commissioner has published a Code of Practice for Users of public area CCTV Systems. A copy of this code may be obtained on application to the Data Protection Commissioner.