CODE OF PRACTICE

For The Operation Of

Long Buckby Parish Council CCTV System

Long Buckby Parish Council is the owner of the CCTV system, and contracts the operation of the system, to Crimesecure Ltd.

Code of Practice for the Long Buckby System based upon The CCTV User Group model code of practice © Copyright

Code of Practice index

Section 1 Introduction and Objectives

1.1 Introduction

A Closed Circuit Television (CCTV) system is operational covering various locations in Long Buckby and its surrounding areas. The system comprises a number of cameras installed at strategic locations. The cameras are fully operational with pan, tilt and zoom facilities. Their images are presented a remote secure Control Room. Secondary monitoring facilities are located at Northamptonshire Police headquarters. Recordings are held securely and are accessible only by qualified operators in the Control Room & Police Headquarters. Images are automatically deleted after a period of 30 days

For the purpose of the document the owner of the system is Long Buckby Parish Council.
For the purpose of the data protection act the Data Controller is the Long Buckby Parish Council. The Parish Clerk is the nominated deputy for the Data Controller'
The 'System Manager' is the Managing Director of Crimesecure Ltd.
The Long Buckby CCTV system has been notified to the Information Commissioner.

*Note 1. The **Data Controller** is the person who (either alone or jointly or in common with other persons) determine the purpose for which and the manner in which any personal data are to be processed, It must be a legal entity e.g. person, organisation or corporate body and in the case of partnership all partners may be considered to bear the responsibility.*

The Parish council being subject to the Human Rights Act, the following conditions apply to its CCTV system.

1.2 Objectives of the system

1.2.1 The objectives of the Long Buckby system as determined by the partnership, which form the lawful basis for the processing of data.

- To help reduce the fear of crime
- To prevent or mitigate interruptions to traffic flow (not to enforce breaches to traffic law)
- To facilitate the apprehension and prosecution of offenders in relation to crime and public order.
- To help detect crime and provide evidential material for court proceedings.
- To assist in the overall management of the village centre and the surrounding areas.
- To assist the local Authority in its enforcement and regulatory functions within the Northamptonshire area.
- To provide safe areas for the benefit of those who live, work, trade, visit, serve and enjoy the facilities and environment of the areas covered by CCTV.

1.3 Operating Procedures Manual

This Code of Practice (hereafter referred as 'the Code') is supplemented by a separate 'Operating Procedures manual', which offers instructions on all aspects of the day-to-day operation of the system. To ensure the Purpose and Principles (see section 2) of the system are realised, the Operating Procedures manual is based and expands upon the contents of this Code of Practice.

Section 2 Statement of Purpose and Principles

2.1 Purpose

The Purpose of this document is to state the intention of the owners and the managers, on behalf of the partnership as a whole and as far as is reasonably practicable, to support the objectives of the Long Buckby CCTV system, (hereafter referred to as 'The System') and to outline how it is intended to do so.

2.1.1 The 'Purpose' of the system, and the process adopted in determining the 'reasons' for implementing 'The System' are as previously defined in order to achieve the objectives detailed within section1.

2.1.2 Whilst Long Buckby Parish Council owns 'The System', representatives from Crimesecure Ltd, staff the control room.

2.2 General Principles of Operation

2.2.1 The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

2.2.2 The operation of the system will also recognise the need for formal authorisation of any covert 'Directed' surveillance of crime – trend (hotspot) surveillance as required by the Regulation of Investigatory Powers Act 2000 and the police force policy.

2.2.3 The system will be operated in accordance with the Data Protection Act 1998 at all times.

2.2.4 The system will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this code, or which are subsequently agreed in accordance with this Code of Practice.

2.2.5 The system will be operated with due regard to the principle that everyone has the right to respect for his her private and family life and their home.

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

2.2.7 Throughout this Code of Practice it is intended, as far a reasonably possible, to balance the objectives of the CCTV system with the need to safeguard the individuals rights. Every effort has been made throughout this code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the system is not only accountable, but it is seen to be accountable.

2.2.8 Participation in the system by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this code and to be accountable under the Code of Practice.

2.3 Copyright

Copyright and ownership of all material recorded by virtue of the system will remain with the data controller

2.4 Camera and area Coverage

2.4.1 The areas covered by CCTV to which this Code of Practice refers are the public areas within the responsibility of the operating partners and cover Long Buckby and its surrounding area, which are as follows:

2.4.2 From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV system and be governed by these codes and procedures.

2.4.3 Some of the cameras offer full colour, pan, tilt, and zoom (PTZ) capability, some of which may switch to monochrome in low light levels.

2.4.4 None of the cameras forming part of the system will be installed in a covert manner. Some cameras may be enclosed within all weather domes for aesthetic or operational reasons, but appropriate signs will identify the presence of all the cameras.

2.5 Monitoring and Recording Facilities

2.5.1 The CCTV control room for the system is operated and staffed by Crimesecure Ltd and referred to as the Crimesecure control room.

2.5.2 Secondary monitoring equipment is located at Northamptonshire Police headquarters based at Wootton Hall Northampton

2.5.3 CCTV operators are able to record images from selected cameras, produce hard copies of recorded images, replay or copy any pre-recorded data, as long as it is in line with this Code of Practice and the Operating Procedures manual.

2.5.4 Requests to review or release images from local authorities or Northamptonshire Police will be carried out by the Crimesecure Ltd. The relevant procedures to carry out the review or release of the footage will be followed at all times.

2.6 Human Resources

2.6.1 Unauthorised persons will not have access to the Crimesecure control room without an authorised member of staff being present.

2.6.2 Specifically selected and trained operators in accordance with the strategy contained within the Operating Procedures manual will staff the control room. All operators of CCTV cameras must be licensed by the Security Industry Authority (SIA).

2.6.3 All licensed operators receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 1998, Regulatory of Investigatory Powers Act 2000 and the codes of practice and procedures.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material, whether recorded digitally, in analogue format, or as a hard copy video print, will be processed and handled strictly in accordance with this Code of Practice and the Operating Procedures manual.

2.8 Operators Instructions

2.8.1 Technical instruction on the use of equipment housed within the Crimesecure control room is contained in a separate manual provided by the equipment suppliers.

2.9 Changes to the Code of Practice or Operating Procedures Manual

2.9.1. Any major changes to either the Code of Practice or Operating Procedures manual, (i.e. such as will have a significant impact upon the Code of Practice or upon the operation of the system) will take place only after consultation with Long Buckby Parish Council, Northamptonshire Police and Crimesecure Ltd.

2.9.2. A minor change (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the system manager and the Clerk of Long Buckby Parish Council.

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 Although a large majority of the public may have become accustomed to being monitored by CCTV, those who do express concerns do so mainly over matters pertaining to the processing of the information, (or data) ie. What happens to the material that is obtained?

3.1.2 All personal data obtained by virtue of the system, shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the system and its code. In processing personal data there will be respect for everyone's right to respect his / her private and family life and their home.

3.2 Data Protection Legislation

3.2.1 The operation of the system has been notified to the office of Information Commissioners in accordance with current data protection legislation.

3.2.2 The CCTV system is registered under the Data Protection Act 1998 within Long Buckby Parish Council and current registrations as follows: - Long Buckby Parish Council (ZA767832).

3.2.3 The 'Data Controller' for the system is Long Buckby Parish Council and day-to-day responsibility for the data will be the Managing Director of Crimesecure Ltd

3.2.4 All data will be processed in accordance with the principles of the Data Protection Act 1998 which, in summarised form, includes, but is not limited to:

- All personal data will be obtained and processed fairly and lawfully.
- Personal data will be held only for the purposes specified.
- Personal data will be used only for the purposes, and disclosed only to the people, shown within this Code of Practice.
- Only personal data will be held which is adequate, relevant and not excessive in relation to the purpose for which the data is held.
- Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.
- Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

3.2.5 Under the Data Protection Act 1998 an individual is entitled to a copy of the information constituting any such data held about him / her. The system managers are not obliged to comply with the request unless he /she is supplied with sufficient information as to reasonably identify the person making the request and to locate the data which the individual seeks.

It is necessary for the individual to formally apply using the 'Subject Access Request Form'. (See 'Procedure for the Release of Evidence' and 'Subject Access Request Form' on the Long Buckby Parish website).

3.2.6 The principles of section 7 and 8 of the Data Protection Act 1998 (Rights of Data subject and others) shall be followed in respect of every request; those sections are produced as Appendix B to this Code.

3.3 Exemptions to the Provision of Information

In considering a request made under the provision of section 7 of the Data Protection Act 1998, reference may also be made to section 29 of the Act which includes, but is not limited to, the following statement:

3.3.1 Personal data processed for any of the following purposes –

- The prevention or detection of crime
- The apprehension or prosecution of offenders

is exempt from the subject access provisions in any case 'to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection'.

Note: Each and every application will be assessed on its own merits and general 'blanket exemptions' will not be applied.

3.4 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 presentation of its own case, (known as unused material). An explanatory summary of the provisions of the Act are contained within the Operational Procedures manual, but disclosure of unused material under the provision of this Act should not be confused with the obligations placed on the data controller by section 7 of the Data Protection Act 19998, (known as Subject Access)

Section 4 Accountability and Public

4.1 The Public

4.1.1 For reasons of security and confidentiality access to the Crimesecure control room is restricted in accordance with the Code of Practice. Visits from members of the public will not be permitted. Any organisation wishing to visit the Crimesecure control room with legitimate reason may be permitted to do so, subject to the approval of the duty staff within the Crimesecure control room.

4.1.2 Cameras will not be used to look into private residential property. Where the system permits it 'Privacy Zones' will be programmed into the system as required in order to ensure that the cameras do not survey the interior of any private residential property within range of the system. If such 'Zones' cannot be programmed the operators will be specifically trained in privacy issues.

4.1.3 A member of the public wishing to register a complaint with regard to any aspect of the system may do so by contacting the Long Buckby Parish Clerk. All complaints will be dealt with under the direction of Long Buckby Parish Council.

4.1.4 Crimesecure control room staff are contractually subject to regulations governing confidentiality and discipline. An individual who suffers damage or distress by reason of any contravention of this Code of Practice may be entitled to instigate legal proceedings.

4.2 System Owner

4.2.1 The Clerk of Long Buckby Parish Council and designated deputy, being the nominated representative of the system owners, will have full and unrestrictive access to the Crimesecure control room and will be responsible for receiving regular and frequent reports from the CCTV Manager.

4.3 System Manager

4.3.1 The nominated manager named at Appendix A will have day-to-day responsibility for the system as a whole.

4.3.2 The system will be subject to an annual review by Long Buckby Parish Council.

4.3.3 The system owner will ensure that every complaint is acknowledged in writing within 10 working days, which will include advice to the complainant of the enquiry procedure to be undertaken. After investigation a formal report will be forwarded to the system owner, giving details of all complaints and the outcome of all-relevant enquires.

4.3.4 Statistical and other relevant information, including any complaints made, may be included in the Annual reports of Long Buckby Parish Council, which will be made available upon request.

4.4 Public Information

4.4.1 A copy of this Code of Practice may be published on Long Buckby Parish Council's website, and a copy will be made available to anyone on request. Additional copies will be lodged at the Long Buckby Library.

4.4.2 Signage

Signs will be placed in the locality of the cameras and at main entrance point to relevant areas covered by CCTV. The signs will indicate:

- The presence of CCTV monitoring
- The 'ownership' of the system
- Contact Telephone number of the 'data controller' of the system.

Section 5 Assessment of the system and the Code of Practice

5.1 Evaluation

5.1.1 The system will periodically be independently evaluated to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The format of the evaluation shall comply with that laid down by the Home Office Statistics and research Directorate in the Home Office Bidding Guidelines and be based on assessments of the inputs, the outputs, the process and the impact of the scheme.

- An assessment of the impact upon crime: This assessment shall include not only the immediate area covered by the cameras but the wider town area, the Policing area, regional areas and national trends.
- An assessment of the incidents monitored.
- An assessment of the impact on town centre business.
- An assessment of neighbouring areas without CCTV.
- The views and opinions of the public.
- The operation of the Code of Practice.
- Whether the purposes for which the system was established are still relevant.
- Cost effectiveness.

5.1.2 The results of the evaluation will be published and will be used to review and develop any alterations to the specified purpose and objectives of the scheme as well as the functioning, management and operation of the system.

5.1.3 It is intended that evaluations should take place at least every 2 years.

5.2 Monitoring

5.2.1 The system manager will accept day-to-day responsibility for the monitoring, operation and evaluation of the system and the implementation of this Code of Practice.

5.2.2 The system manager shall also be responsible for maintaining full management information as to the incidents dealt with by the control room, for use in the management of the system and in future evaluations.

5.3 Audit

5.3.1 The organisation's auditors or other appropriate person, or his/her nominated deputy, who is not the system manager, will be responsible for regularly auditing the operation of the system (annually) and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examinations of the monitoring room records, recorded image histories, and the content of recorded material.

5.4 Inspection

5.4.1. Inspections will be carried out by an approved organization as agreed by Long Buckby Parish Council. The inspector will be permitted access to the Crimesecure control room, without prior notice and to the records held therein at any time, provided their presence does not disrupt the operational functioning of the room.

Section 6 Human Resources

6.1 Staffing of the Crimesecure Control Room and those responsible for the day-to-day operation of the system.

6.1.1 The Crimesecure control room will be staffed in accordance with the Operating Procedures manual. The operators of the system are employed by the monitoring contractor and are subject to their disciplinary procedures. The system will only be operated by authorised personnel who will have been properly trained in its use and all control room procedures.

6.1.2 All operators of the system must be in the possession of a valid SIA CCTV Licence.

6.1.3 Every person involved in the management and operation of the system will be personally issued with a copy of the Code of Practice and the Operating Procedures manual, and will be required to sign a confirmation that they fully understand the obligations adherence to these documents, and any breach will be considered as a disciplinary offence by Crimesecure Ltd. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he / she will be expected to comply with as far as is reasonably practicable at all times.

6.1.4 Arrangements may be made for a police liaison officer to be present in the Crimesecure control room at certain times, or indeed at all times. If this was to be the case the officer must not interfere with the operation in anyway and would be there solely for liaison purposes. The officer will not be allowed to control the cameras in accordance with the Code of Practice and Operating Procedures manual.

6.1.5 All personnel involved in the system shall receive training from time to time in respect of all legislations appropriate to their role / duties. The system manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has day-to-day responsibility for the management of the control room and for enforcing the discipline rules. Non-compliance with this Code of Practice by any person will be considered a severe breach of discipline and dealt with accordingly, including, the instigation of criminal proceedings.

6.2 Declaration Of Confidentiality

6.2.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the system to which they refer, will be required to sign a declaration of confidentiality (see example at appendix E)

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

7.1.1 Any person operating the cameras will act with the utmost probity and awareness at all times.

7.1.2 At least one operator must be present within the Crimesecure control room throughout operating hours. Camera surveillance must be maintained throughout. Operating times are subject to agreement with the system owners.

7.1.3 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.

7.1.4 Every use of the cameras will accord with the purposes and key objectives of the system and shall be in compliance with this Code of Practice.

7.1.5 Cameras will not be used to look into private residential property. 'Privacy zones' shall be programmed into the system (whenever practically possible) in order to ensure that the interior of any private residential property within the range of the system cannot be surveyed by the camera.

7.1.6 Camera operators will be mindful of exercising prejudices, which may lead to complaints of the system being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the system or by the system manager.

7.1.7 It is necessary for the control room staff to be made aware of the purpose for which the cameras are required to ensure that the request is in line with the Code of Practice and legislations.

7.2 Primary Control

7.2.1 Only those trained and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times.

7.2.2 In the case of a major incident, the police may assume control within the Crimesecure control room. This will be subject to a formal request being made to Crimesecure Ltd in the first instance, and subsequent approval of Long Buckby Parish Council and Crimesecure Ltd. It is important however, that the monitoring controls are handled by the duty controllers or under their direction to maintain maximum efficiency.

7.3 Secondary Controls

7.3.1 No secondary controls or recording equipment are installed.

7.3.2 Secondary monitoring facilities are provided at Northamptonshire Police Headquarters.

7.4 Operation of The System by the Police

7.4.1 Under extreme circumstances the police may request to assume control of the system to which the Code of Practice applies. Only requests made on the written authority of a police officer not below rank of Inspector will be considered. Any such request will only be accommodated on the personal written authority of the most senior available representative of the system owners.

7.4.2 In the event of such a request being permitted, the Crimesecure control room will continue to be staffed, and equipment operated by, only those personnel who are authorised to do so, who will then operate under the direction of the police officer designated in the written authority.

7.4.3 In very extreme circumstances a request may be made for the police to take total control of the system in its entirety, including the staffing of the control room and personal control of all associated equipment, to the exclusion of all representatives of the system owners. Any such request should be made to the system manager in the first instance, which will consult personally with the most senior officer of the system owners (or designated deputy of equal standing). A request for total exclusive control must be made in writing by a police officer not below rank of Assistant Chief Constable or person of equal standing.

7.5 Maintenance of the system

7.5.1 To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality, the system shall be maintained in accordance with the requirements of the Operating Procedures manual under a maintenance agreement.

7.5.2 The maintenance agreement is a confidential document agreed between Long Buckby Parish Council and Crimesecure Ltd.

7.5.3 It is the responsibility of the system manager to ensure appropriate records are maintained in respect of the functioning of the cameras, and monitoring equipment reporting to the system owners as agreed.

Section 8 Access to, and Security of, Control Room and Associated equipment

8.1 Authorised use of the CCTV system

8.1.1 Only trained and authorised personnel will operate any of the equipment located within the Crimesecure control room, (or equipment associated with the CCTV system).

8.2 Access

8.2.1 During operational hours the Crimesecure control room staff will manage access to the complex. Controllers must satisfy themselves of the identity of the caller and the purpose of their visit before allowing access.

8.2.2 General access to the Crimesecure control room will be strictly limited by access control to duty controllers, and persons employed by or contracted to Crimesecure Ltd.

8.2.3 Outside of operational hours access to the Crimesecure control room will be managed by Crimesecure staff

8.2.4 All persons accessing the control room **must** complete the access log.

8.3 Public Access

8.3.1 Public access to the Crimesecure control room will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the system manager. Any such visits will be conducted and recorded in accordance with the Operating Procedures manual.

8.3.2 Routine visits to the Crimesecure control room (other than by on duty police staff for legitimate reasons and by the System Owner by prior agreement) will not be permitted.

8.4 Authorised Visits

8.4.1 Visits by inspectors or auditors do not fall into the scope of the above paragraph and may take place at any time, without prior warning. No more than (two) inspectors or auditors will visit at any one time. Inspectors or Auditors will not influence the operation of any part of the system during their visit. The visit will be suspended in the event of it being operationally inconvenient. Any such visit should be recorded in the log.

8.5 Declaration of Confidentiality

8.5.1 Regardless of their status, all visitors to the Crimesecure control room, including inspectors and auditors, will be required to sign the visitor's log and a declaration of confidentiality.

NOTE: Every visitor to the Crimesecure Control Room must sign the visitors book thereby making the declaration:-

'In signing this visitors book all visitors to the Crimesecure control room acknowledge that the precise location of the Crimesecure control room and personal details of those operating the system, is, and should remain confidential. They further agree not to divulge any information obtained, overheard or overseen during their visit'

8.6 Security

8.6.1 Authorised personnel will normally be present at all times when equipment is in use. If the control room is to be left unattended for any reason it will be secured. In the event of the control room having to be evacuated for safety or security reasons, the provisions of the Operating Procedures manual will be complied with.

8.6.2 The Crimesecure control room will at all times be secured with appropriate access control.

Section 9 Management of Recorded Material

9.1 Guiding Principles

9.1.1 For the purposes of this Code ' recorded material' means any material recorded by, or as a result of, technical equipment which forms part of the system, but specially includes images recoded digitally, or on videotape or by way of video copying, including video prints.

9.1.2 Every video or digital recording obtained using the system has the potential of containing material that has to be admitted in evidence at some point during its life span.

9.1.3 Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of the system, will be treated with due regard to their individual right to respect for their private and family life.

9.1.4 It is therefore of the utmost importance that irrespective of the means of format (e.g. paper copy, video tape, digital tape, CD, or any form of electronic processing and storage) of the images obtained by the system, they are treated strictly in accordance with this Code of Practice and the procedural manual from the moment they are received by the control room until final destruction. Every movement of usage will be meticulously recorded.

9.1.5 Access to and the use of recorded material will be strictly for the purposes defined in this Code of Practice only.

9.1.6 Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

9.1.7 If at the request of the police recorded material is to be released to the media to assist in the apprehension, prosecution of offenders / or assist them with enquires, then a written request should be received from a police officer of a rank no less than a superintendent and written authority be granted by the senior officer of the system owners (or designated deputy of equal standing).

9.2 National standard for the release of data to a third party

9.2.1 Every request for the release of personal data generated by this CCTV system will be channeled through the system manager. The system manager will ensure the principles contained within Appendix B to this Code of Practice are followed at all times.

9.2.2 In complying with the National standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles.

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice.
- Access to recorded material will only take place in accordance with the standards outlined in appendix B and this Code of Practice.

- The release or disclosure of data to commercial or entertainment purposes is specifically prohibited.

9.2.3 Members of the police service or other agency having a statutory authority to investigate and / or prosecute offences may, subject to compliance with appendix C, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded in accordance with the Operating Procedures manual.

NOTE; *Release to the media of recorded information, in whatever format, which may be part of a current investigation would be covered by the Police and Criminal Evidence Act, 1984. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial. Full details of any media coverage must be recorded and brought to the attention of both the Prosecutor and the Defence.*

9.2.4 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix B and the Operating Procedures manual.

9.2.5 It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of the CCTV system, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of this CCTV system will only be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

9.3 Digital Recorders

9.3.1 All CCTV cameras recorded by the system are digitally recorded on to dedicated digital video recorders. All images are stored on the recorders hard drive, for the time period specified in the Operating Procedures manual, and only viewed, downloaded, re-produced when the operators are requested to do so by the police or the system owners, and only in accordance with the Operating Procedures manual.

9.4 Image Retention

9.4.1 Recorded footage will be retained for a period of one calendar month. The digital recorders will automatically erase any footage that is over 31 days old.

9.4.2 Digital footage will always be used and stored in accordance with the Operating Procedures manual. At the conclusion of their life within the CCTV system it will be destroyed in accordance with the manual and the destruction logged and certified.

9.5 Digital Recorder register

9.5.1 Each CD/DVD produced will be given a unique tracking record maintained in accordance with the Operating Procedures manual. The tracking record will be retained for at least 3 years after the CD/DVD has been destroyed. The tracking record shall identify every use, and details of every person who has viewed or had access to the media disc from production, storage, through to its final destruction.

9.6 Recording Policy

9.6.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period at a frame rate of 4 images per second, on to multiple 16 channel digital recorders. The images recorded will be stored on the hard drive of the recorder for no longer than 31 days. The recorder will automatically erase any images over 30 days old.

9.6.2 Dedicated spot monitors are in use to record images that the operators select on to their monitors. Images will be recorded in real time at a frame rate of 25 frames per second, and stored on the recorders hard drive for a maximum of 30 days. The recorder will automatically erase any images over 30 days old.

9.6.3 In the event images recorded on the digital recorders are required for evidential purposes the procedures outlined in the Operating Procedures manual will be strictly complied with.

Section 10 Video Print

10.1 Guiding Principles

10.1.1 A video print is a copy of an image or images which already exist on videotape / computer disc. Such prints are equally within the definitions of 'data' and recorded material.

10.1.2 Video print will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator, who will be responsible for recording the full circumstances under which the print is taken, in accordance with the Operating Procedures manual.

10.1.3 Video prints contain data and will therefore only be released under the terms of Appendix B to this Code of Practice. 'Release of data to third parties'. If prints are released to the media, (in compliance with Appendix B), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Operating Procedures manual.

10.1.4 A record will be maintained of all video print productions in accordance with the Operating Procedures manual. The recorded details will include: a sequential number, the date, time and location of the incident, date and time of the production of the print and the identity of the person requesting the print, (if relevant) and the purpose for which the print was taken.

10.1.5 The record of the video print taken will be subject to audit in common with all other records in the system.

10.1.6 Video prints will not be issued to security staff, or members of any radio link scheme.

Appendix A Key Personnel and Responsibilities

1. System Owner & Data Controller

Long Buckby Parish Council **Tel: 01327 301570**

Designated Representative
Parish Clerk
3 Packwood Close
Daventry
NN11 8AJ

Representative's Deputy
R Vivian (Cllr.)

2. Monitoring Contractor

Crimesecure Ltd
Address withheld

Responsibilities:

Long Buckby Parish Council is the 'Owner' of the system.
The Managing Director of Crimesecure Ltd, (The System Manager) will be the single point of reference for operational maters on behalf of the owners. His role will include a responsibility to:

- Ensure the provision and maintenance of all equipment forming part of the system in accordance with contractual arrangements, which the owners may from time to time enter into.
- Maintain close liaison with representatives of the system owners and Northamptonshire Police.
- Ensure the interests of the operational partners and other organisations are upheld in accordance with the terms of this Code of Practice.
- Agree to any proposed alterations and additions to the system, this Code of Practice and / or the Operating Procedures manual.
- Executive for operational strategy and policy.
- Authority for sole occupation of Crimesecure control room by Police.

The System Manager
Managing Director
Crimesecure Ltd **Tel: 01327 310361**

4. CCTV Manager

The CCTV Manager is the 'Manager' for the Long Buckby system. He has delegated authority for data control on behalf of the 'data controller' His roles are as follows:

Responsible for:

- Operational responsibility for the day-to-day operation of the CCTV system. Day to day liaison with Northamptonshire Police.
- Day to day liaison and supervision of duty controllers
- Day to day liaison with system owner for authorisation of repairs, goods, and service
- Day to day liaison with maintenance contractors.
- Day to day liaison with CCTV partners.
- Managing the monitoring contract, and staff.
- Site Health & Safety.
- Ensuring Compliance with this Code of Practice.

CCTV Manager
Managing Director
Crimesecure Ltd **Tel: 01327 310361**

Appendix B Extracts from the Data Protection Act 1998

Section 7

(1) Subject to the following provisions of this section and to section 8 and 9, an individual is entitled:

(a) To be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

(b) If that is the case, to be given by the data controller a description of -

(i) The personal data of which that individual is the data subject.
(ii) The purpose for which they are being or are to be processed.
(iii) The recipients or classes of recipients to whom they are or mat be disclosed.

(c) To have communicated to him/her in an intelligible form.

(i) The information constituting any personal data of which that individual is the data subject;

(ii) Any information available to the data controller as the source of those data;

(d) Where the processing by automatic means of personal data of which that individual is the data subject for the purposes of evaluating matters relating to him/her such as, for example, his/her performance at work, his/her creditworthiness, his/her reliability or his/her conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him/her, to be informed by the data controller of the logic involved in that decision – taking.

(2) A data controller is not obliged to supply any information under subsection (1) unless he/she has received.

(a) A request in writing

(b) Except in prescribed cases, such fee (not exceeding the prescribed maximum) as he/she may require.

(3) A data controller is not obliged to comply with a request under the section unless he/she is supplied with such information as he/she may reasonably require in order to satisfy him/herself as to the identity of the person making the request and to locate the information which that person seeks.

(4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he/she is not obliged to comply with the request unless:

(a) The other individual has consented to the disclosure of the information to the person making the request, or

(b) It is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing the data controller from communicating so much information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.

(6) In determining for the purpose of subsection (4) (b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:

(a) any duty of confidentiality owed to the other individual.
(b) any steps taken by the data controller with a view to seeking the consent of the other individual,
(c) whether the other individual is capable of giving consent. And
(d) any express refusal of consent by the other individual.

Note: In considering such instances the data controller must effectively also consider the degree of privacy that the third parties might or might not reasonably expect in being at that location at that time.

(7) An individual making a request under this section may, in such cases as may be prescribed, specify that his/her request is limited to personal data of any prescribed description.

(8) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

(9) If a court is satisfied on the application of any person who has made a request under the forgoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him/her to comply with the request.

In this section:
'Prescribed' means prescribed by the secretary of state by regulations;

'The prescribed maximum' means such amount as may be prescribed;

'The prescribed period' means forty days or such other period as may be prescribed.

'The relevant days', in relation to a request under this section, means the day of which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3)

(10) Different amounts or periods may be prescribed under this section in relation to different cases.

Section 8

(1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provisions of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.

(2) The obligation imposed by section 7 (1) (c) (i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:

(a) The supply of such a copy is not possible or would involve disproportionate effort, or
(b) The data subject agrees otherwise.
(c) And any of the information referred to in section 7 (1)(c)(i) is expressed in terms, which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regards shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

(5) Section 7 (1) (d) is not to be regarded as requiring the provision of information as to the logic involved in decision-making if, and to the extent that, the information constitutes a trade secret.

(6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take into account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the request.

(7) For the purpose of section 7 (4) and (5) another individual can be identified from the information being requested from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

Appendix C National Standard for the release of data to third parties

1. Introduction

Arguably CCTV is one of the most powerful tools to be developed during recent years to assist efforts to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems are to command the respect and support of the general public, the systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

Long Buckby Parish Council is committed to the belief that everyone has the right to respect for his or her private and family life and their home. Although the use of CCTV cameras has become widely accepted in the UK as an effective tool, those people who do express concern tend to do so over the handling of the information (data), which the system gathers.

After considerable research and consultation the system owners have adopted the nationally recommended standard of The CCTV User Group.

2. General Policy

All requests for the release of data shall be processed in accordance with the Operating Procedures manual. All such requests shall be channeled through the data controller.

Note: The *data controller* is the person who (either alone or jointly with others) determines the purpose for which and the manner in which any personal data are, or are not to be processed.

(In most cases the data controller is likely to be the scheme owners or for a 'partnership' the partners share responsibility)
Day to day responsibility may be devolved, usually to the scheme manager.

3. Primary Request to View Data

a) Primary requests to view data generated by the CCTV system are likely to be made by third parties for any one or more of the following purposes.

- Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & investigations Act 1996, etc).
- Providing evidence in civil proceedings or tribunals.
- The prevention of crime.
- The investigation and detection of crime (may include identification of offenders).

- Identification of witnesses.

b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

- Police.
- Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
- Solicitors.
- Accused persons or defendants in criminal proceedings.
- Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status.

c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:

- Not unduly obstruct a third party investigation to verify the existence of relevant data.
- Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.

Note: A time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data, (e.g. a time limit was about to expire)

d) In circumstances outlined in note (3) below, (requests by plaintiffs, accused Persons or defendants) the data controller, or nominated representative, shall:

- Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
- Treat all such enquiries with strict confidentiality.

Notes

(1) The release of data to the police is not to be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (it may be appropriate to put in place special arrangements in response to local requirements).

(2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.

(3) There may be occasions when an enquiry by a plaintiff, an accused person, a Defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

(4) The data controller shall decide which (if any) "other agencies" might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this standard.

(5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest ½ hour.

4. Secondary Request to View Data

A) A 'secondary' request for access to data may be defined as any request being made that does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:

(a) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data protection act 1998, Human rights act 1998, Section 163 Criminal Justice and Public Order Act 1994 etc.)

(b) Any legislation requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998)

(c) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and

(d) The request would pass a test of 'disclosure in the public interest'.

B) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:

(a) In respect of material to be released under the auspices of 'crime prevention', written agreements to the release of the material should be obtained from a police officer, not below the rank of Chief inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice.

(b) If the material is to be released under the auspices of 'public well being, health and safety', written agreement to the release of material should be obtained from a senior officer within the local authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.

C) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

5. Individual Subject Access under Data Protection Legislation

1) Under the terms of Data Protection Legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:

i) The request is made in writing.

ii) A specified fee is paid for each individual search;

iii) The data controller is supplied with sufficient information to satisfy him or herself as to the identity or the person making the request;

iv) The person making the request is only shown information relevant to that particular search and which contains personal data for her or himself only, unless all other individuals who may be identified from the same information have consented to the disclosure.

2) In the event of the data controller complying with a request to supply a copy of the data of the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any person should be concealed or erased). Under these circumstances an additional fee may be payable.

3) The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however every effort should be made to comply with subject access procedures and each request should be treated on its own merits.

4) In addition to the principles contained within the data protection legislation, the data controller should be satisfied that the data is:

i) Not currently and, as far as can be reasonably ascertained, not likely to become part of a 'live' criminal investigation;

ii) Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;

iii) Not the subject of a complaint or dispute which has not been actioned;

iv) The original data and that the audit trail has been maintained;

v) Not removed or copied without proper authority;

vi) For individual disclosure only (i.e. to be disclosed to a named subject)

6. Process of Disclosure:

a) Verify the accuracy of the request.

b) Replay the data to the requestee only, (or responsible person acting on behalf of the person making the request).

c) The viewing should take place in a separate room and not in the control or monitoring area. Only data that is specific to the search request shall be shown.

d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out either by means of electronic screening or manual editing on the monitor screen).

e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

NOTE: The Information Commissioners Code of Practice for CCTV makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.

7. Media disclosure

Set procedures for release of data to a third party should be followed, if the means of editing out other personal data does not exist on site, measures should include the following:

a) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use

b) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities / data that must not be revealed.

c) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection Legislation and the system's Code of Practice).

d) The release form shall be considered a contract and signed by both parties.

8. Principles

In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the CCTV scheme;

b) Access to recorded material shall only take place in accordance with this standard and the Code of Practice.

c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Any 'partners' to a CCTV system should all sign and certify their commitment to abide by these codes at all times whilst involved with the scheme.

Code of Practice in respect of the Operation of

Long Buckby Parish Council CCTV System

Agreed by

Long Buckby Parish Council, Northamptonshire Police, and Crimesecure Ltd

Certificate of Agreement

The content of both this Code of Practice and the Operating Procedures manual are hereby approved in respect of the Long Buckby Closed Circuit Television System and, as far as reasonably practicable, will be complied with by all who are involved in the management and operation of the system.

Signed for and on behalf of Long Buckby Parish Council

Signature: ……

Name: …… Position held: ……

Dated the……day of……20…

Signed for and on behalf of Crimesecure Ltd.

Signature……

Name…… Position held……

Dated the……day of……20…

Amendments: Nil