Fenland District Council & Peterborough City Council CCTV shared service

Codes of Practice

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect of the Peterborough City Council and Fenland District Councils CCTV shared service and, as far as is 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 *Fenland District Council*

Signature: .....….....

Name: ……. Position held: ……

Dated the .....……. day of ..... 20…

Signed for and on behalf of *Peterborough City Council*

Signature: .....….....

Name: ……. Position held: ……

Dated the .....……. day of ..... 20…

Signed for and on behalf of *Cambridgeshire Constabulary*

Signature: .....….....

Name: ……. Position held: ……

Dated the .....……. day of ..... 20…

Section 1 Introduction and Objectives

1. Introduction

1.1 Background to CCTV

1.1.1 A Public Spaces Closed Circuit Television (CCTV) system operates in both Fenland District Council and Peterborough City Councils geographical areas. This system, known as the CCTV shared service, comprises of a number of cameras installed at strategic locations. The majority of the cameras are fully operational with pan, tilt and zoom facilities and are monitored from the Council's CCTV shared service purpose built control room located in Peterborough.

1.1.2 Others are fixed cameras, images from which are presented in the same room. This Code of Practice does not extend to the use and operation of cameras held by other internal services & teams for the purpose of covert surveillance.

1.1.3 The CCTV shared service has evolved from the formation of a partnership ('the Partnership') between Peterborough City Council and Fenland District Council who have all certified on the previous form their acceptance of the requirements of this code. The shared service between both Fenland District Council and Peterborough City Council was established from the 1st January 2020.

1.1.4 For the purposes of this document, the 'owner' of the system is Peterborough City Council and Fenland District Council.

1.1.5 For the purposes of the Data Protection Act the 'data controller' is Peterborough City Council and Fenland District Council.

1.1.6 The CCTV shared service has been notified to the Information Commissioner as required by the Data Protection Act 2018.

1.1.7 Details of key personnel, their responsibilities and contact points are shown at Appendix A to this Code.

1.2 Partnership statement in respect of The Human Rights Act 1998

1.2.1 The partnership recognises that public authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998, and consider that the use of CCTV in Peterborough and Fenland is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

1.2.2 This assessment is evidenced by an agreed 'operational requirement' document (and any survey or consultation where applicable). Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by the Partnership towards their duty under the Crime and Disorder Act 1998.

1.2.3 It is recognised that operation of the shared service CCTV System may be considered to infringe on the privacy of individuals. The partnership recognise that it is their responsibility to ensure that the scheme should always comply with all relevant legislation, to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic well-being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.

1.2.4 The Codes of Practice and observance of the Operational Procedures Manual shall ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for everyone's right to a free trial.

1.2.5 The shared service CCTV System shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.3 Councils aims and objectives

1.3.1 The following are the aims and objectives of Fenland District Council & Peterborough City Council's CCTV Scheme:

1.3.1.1 A reduction in the fear of crime and reassurance of the public;

1.3.1.2 To help secure a safe environment for those that live, work or trade in the district and City and those who visit the area.

1.3.1.3 The detection, deterrence and prevention of crime including:

1.3.1.4 Providing assistance in the prevention of crime;

1.3.1.5 Deterring and detecting crime;

1.3.1.6 Helping to identify, apprehend and prosecute offenders;

1.3.1.7 Providing the Police with evidence to take criminal action in the courts;

1.3.1.8 Gathering of criminal intelligence.

1.3.1.9 The maintenance of public order by assisting with:

1.3.1.9.1 Improving the Town and City environments;

1.3.1.9.2 Regeneration initiatives to improve the quality of life;

1.3.1.9.3 The implementation of the Crime and Disorder strategies made under the Crime and Disorder Act 1998;

1.3.1.9.4 The implementation of the Clean Neighbourhoods and Environment Act 2005;

1.3.1.9.5 Evidence of moving and stationary traffic and excise offences.

1.3.1.10 **The key objectives of the system are:**

1.3.1.11 To help reduce the level of crime, vandalism and public disorder;

1.3.1.12 To detect, prevent or reduce the incidence of property crimes and offences against the person;

1.3.1.13 To improve communication and the operational response of Police patrols;

1.3.1.14 To help reduce vehicle crime and improve general security in car parks;

1.3.1.15 To improve and enhance public safety, both in terms of personal security and security of buildings and premises;

1.3.1.16 To help make the Town and City centre a better area to shop, work and visit;

1.3.1.17 To help reduce anti-social behaviour;

1.3.1.18 To monitor major events such as carnivals and fairs and other visitor attractions, that may take place within the Town Centre and surrounding areas.

1.3.1.19 To assist in the management of the Fenland District Council and Peterborough City Council town centres as well as the villages and rural areas within their responsibility.

1.3.1.20 To support local business against crime schemes with CCTV and radio support.

1.3.3 Within this broad outline, the Partnership has drawn up, and published specific key objectives (which will be reviewed annually) based on local concerns.

1.4 Procedural Manual

1.4.1 This Code of Practice (hereafter referred to as 'the Code') is supplemented by separate internal 'Operational Procedure Manuals' (OPM) 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 CCTV system are realised, the OPM is based and expands upon the contents of this Code of Practice.

Section 2 Statement of Purpose and Principles

2.1 Purpose

2.1.1 This Code of Practice is to regulate the operation of Fenland District Council and Peterborough City Council's shared service Closed Circuit Television (CCTV) systems operating within Fenland and Peterborough City and to set out the rules to be observed by the Councils, its Members, employees, and contractors; the Police and any other party or organisation involved in the management, operation and administration of the CCTV system.

2.1.2 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 Section 1.

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 surveillance that falls within the definition of 'Directed Surveillance' under the Regulation of Investigating Powers Act 2000 (see Appendix G).

2.2.3 The system will be operated in accordance with the Data Protection Act 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 which 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 or 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 as reasonably possible, to balance the objectives of the CCTV System with the need to safeguard the individual's rights. Every effort has been made throughout the 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 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

2.3.1 Copyright and ownership of all material recorded by virtue of The System will remain with the data controller for each respective council.

2.4 Cameras 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 the Fenland District and Peterborough City areas.

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 The majority of cameras have pan tilt and zoom (PTZ) operation, and whilst all have full colour capability some may automatically switch to monochrome in extremely low light conditions.

2.4.4 There are various types of digital cameras to meet the operational requirements in each area. The images from the cameras are digitally recorded and fed back to the control room either by fibre optic cable or via a dedicated and secure wireless transmission.

2.4.5 All cameras are clearly identifiable and have signs indicating who is operating them and how the system owners can be contacted.

2.4.6 The partnership will not use dummy or covert cameras, or cameras which can monitor sound.

2.4.4 None of the cameras forming part of the System will be installed in a covert manner. The presence of CCTV cameras will be identified by appropriate signs.

2.4.5 A map showing the number and location of all fixed cameras is available for inspection and is available via the Peterborough City Council website. Locations of cameras covering FDC can be made available on request but in the main cover the four market towns of Chatteris, March, Whittlesey and Wisbech.

2.5 Monitoring and Recording Facilities

2.5.1 The monitoring of the system is carried out at the purpose built CCTV shared service control room which is located at Sand Martin House (SMH), Peterborough. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.

2.5.2 Secondary monitoring equipment may be located in police premises and within council operated highways control centres. No equipment, other than that directly connected to the main CCTV control room shall be capable of recording images from any of the cameras.

2.5.3 CCTV operators are able to record images from selected cameras in real-time, produce hard copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised users.

2.5.4 Remote control of camera movements is not permitted except at the designated Business Continuity Plan (BCP) satellite CCTV site by CCTV staff who will staff the location if required.

2.5.5 The CCTV control room will be operational 24 hours a day, 365 days per year.

2.5.6 The control room will be staffed by at least one operator at all times throughout the full operational period. Exceptions will be sudden staff sickness, power supply failure, fibre optic or wider system failure and disaster impacting upon SMH.

2.6 Human Resources

2.6.1 The CCTV service will be managed by the CCTV shared service manager, and the monitoring room shall be staffed by specially selected and trained PCC operators in accordance with the strategy contained within the procedural manual.

2.6.2 Unauthorised persons will not have access to the CCTV Control Room without an authorised member of staff being present.

2.6.3 All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 2018, General Data Protection Regulation 2018, Regulation of Investigatory Powers Act 2000, Surveillance Camera Code of Practice and the Codes of Practice and Procedures. Further training will be provided as necessary.

2.6.4 All CCTV operators and the CCTV manager will be licensed with the Security Industry Authority for Public Space Surveillance.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material will be processed and handled strictly in accordance with this Code of Practice and internal OPM.

2.8 Operators Instructions

2.8.1 Technical instructions on the use of equipment housed within the monitoring room are contained in a separate manual provided by the equipment suppliers.

2.9 Changes to the Code or the Procedural Manual

2.9.1 Any major changes to either the Code of Practice or OPM, (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, and upon the agreement of all organisations with a participatory role in the operation of the system.

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 manager and the owners of the system.

2.9.3 Contributors to the Code of Practice

2.9.3.1 The original Code of Practice, which existed in individual form for FDC and PCC was prepared in consultation between the Councils and the Police.

2.9.4 Future Revision and Consultation

2.9.4.1 This Code of Practice will be subject to regular reviews, at least annually.

2.9.4.2 This Code is supported by internal Operating Procedures Manuals (OPM). The OPM is a restricted document and are for the use of CCTV staff only.

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 Although the majority of the public at large may have become accustomed to the use of CCTV cameras, those who do express concern do so mainly over matters pertaining to the processing of the information, (or data) i.e. what happens to the material that is obtained.

Note: '**Processing'** means **obtaining, recording** or **holding** the information or data or **carrying out any operation** or **set of operations** on the information or data, including;

i) Organisation, adaptation or alteration of the information or data;
ii) Retrieval, consultation or use of the information or data;
iii) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
iv) Alignment, combination, blocking, erasure or destruction of the information or data.

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. In processing personal data there will be total respect for everyone's right to respect for his or her private and family life and their home.

3.1.3 The storage and security of the data will be strictly in accordance with the requirements of the General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018 (DPA 2018) herewith referred to as data protection legislation and additional locally agreed procedures.

3.2 Data Protection Legislation

3.2.1 The operation of The System has been notified to the Office of the Information Commissioner in accordance with current Data Protection legislation.

3.2.2. The 'data controller' for The System' is Peterborough City Council & Fenland District Council and day to day responsibility for the data will be devolved to the CCTV shared service manager.

3.2.3 All data will be processed in accordance with the principles of data protection legislation which, in summarised form, includes, but is not limited to:

i) All personal data will be obtained and processed fairly and lawfully.
ii) Personal data will be held only for the purposes specified.
iii) Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.
iv) Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date.
v) Personal data will be held for no longer than is necessary.
vii) 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.

Additionally, individuals will have the rights accorded to them under data protection legislation and be able to exercise these. Personal data will be used only for the purposes as described in this policy, and disclosed only to the people or parties, shown within these codes of practice.

3.3 Request for information (subject access)

3.3.1 Any request from an individual for the disclosure of personal data which he/she believes is recorded by virtue of the system will be directed in the first instance to the system manager or data controller.

3.3.2 The principles of Articles 15 to 21 of the GDPR regarding rights of data subjects shall be followed in respect of every request with due regard to Schedule 2 of the DPA 2018.

3.3.3 If the request cannot be complied with without identifying another individual, permission from all parties will be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.

3.3.4 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Subject Access' request form is included in Appendix F.

3.4 Request for CCTV data by agencies other than Statutory Prosecuting Agencies (SPA's)

3.4.1 If, in exceptional circumstances, the release of recorded data is requested by agencies other than SPA's, such a release will only be granted on the authority of the CCTV shared service manager. The procedures for requesting, handling and logging the recorded data are as described for the release to SPA's, however commercial agents such as insurance companies shall be charged a fee of at least £100 to cover administration costs.

3.4.2 Any personal data requests from members of the general public or a third party will be dealt with under the provisions of the General Data Protection Regulations Act, or the Freedom of Information Act 2000 and follow council processes. Further information is available on the respective Council's website.

3.5 Exemptions to the Provision of Information

3.5.1 In considering a request made under the provisions of Article 15 of the GDPR reference may also be made to Schedule 2, Part 1 ((2) Act which includes, but is not limited to, the following statement:
Personal data processed for any of the following purposes -
i) The prevention or detection of crime
ii) The apprehension or prosecution of offenders
Are 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'.

3.6 Data Protection Impact Assessments (DPIA)

3.6.1 The existing CCTV systems for both FDC and PCC have been subject to a DPIA and any new cameras or changes to current cameras, e.g. in terms of capabilities, then a DPIA will be completed.

Section 4 Accountability and Public Information

4.1 The Public

4.1.1 For reasons of security and confidentiality, access to the CCTV monitoring room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, Partners wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the manager of the System.

4.1.2 Cameras will not be used to look into private residential property. Where the equipment permits it, 'Privacy zones' will be programmed into the system as required in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras. 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 System Manager’s office. All complaints shall be dealt with in accordance with respective council’s complaints procedure, a copy of which may be obtained from Peterborough Direct at the Town Hall or from Fenland Hall, March. Any performance issues identified will be considered under the organisations disciplinary procedures to which all members of Peterborough City Council, including CCTV personnel, are subject.

4.1.4 All CCTV staff are contractually subject to regulations governing confidentiality and discipline. An individual who suffers damage by reason of any negligent contravention of this Code of Practice may be entitled to compensation.

4.2 System Owner

4.2.1 The Director of People and Communities, being the nominated representative of the system owners for Peterborough City Council, and the Director of Housing and Community Support, being the nominated representative of the system owners for Fenland District Council, will have unrestricted personal access to the CCTV monitoring room and will be responsible for receiving regular and frequent reports from the manager of the system.

4.2.2 Peterborough City Council has nominated the Audit Committee with the prime responsibility for receiving and considering those reports. However, if appropriate to the service, other Panels may be consulted including from Fenland District Council.

4.2.3 Formal consultation will take place between the owners and the managers of the system with regard to all aspects, including this Code of Practice and the OPM.

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 manager will ensure that every complaint, on behalf of each council, is acknowledged in writing within five working days which will include advice to the complainant of the enquiry procedure to be undertaken. A formal report will be forwarded to the nominee of the system owner named at Appendix A, giving details of all complaints and the outcome of relevant enquiries.

4.3.3 Statistical and other relevant information, including any complaints made, will be included in the Annual Reports of Peterborough City Council and Fenland District council, which are made publicly available.

4.4 System Development

4.4.1 The Safer Peterborough Partnership (SPP) and the Fenland Community Safety Partnership (FCSP) provides an advisory role for the development of these services and the strategic fit within the Community Safety strategy.

4.4.2 The development and physical infrastructure is advised by the Council's executive decision-making structure.

4.5 Public Information

4.5.1 Code of Practice

A copy of this Code of Practice shall be published on Peterborough City Council and Fenland District Council CCTV web pages, and a copy will be made available to anyone on request.

4.5.2 Signs

Signs (as shown below) will be placed in the locality of the cameras. The signs will indicate:

i) The presence of CCTV monitoring;
ii) The 'ownership' of the system;
iii) Contact telephone number of the 'data controller' of the system.

Section 5 Assessment of the System and 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 assessment of The Inputs, The Outputs, The Process and the Impact of the scheme.

i) 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 Police Divisional and regional areas and national trends.
ii) An assessment of the incidents monitored by the system
iii) An assessment of the impact on town centre business
iv) An assessment of neighbouring areas without CCTV
v) The views and opinions of the public
vi) The operation of the Code of Practice
vii) Whether the purposes for which the system was established are still relevant
viii) 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 two years and national benchmarking data will be compared where appropriate.

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 monitoring room, for use in the management of the system and in future evaluations.

5.3 Audit

5.3.1 The Director of People and Communities (PCC) and/or the Director of Housing and Community Support (FDC), who is not the system manager, will be responsible for regularly auditing the operation of the system and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of the monitoring room records, data histories and the content of recorded material.

5.3.2 Financial management of the CCTV shared service will be subject to inspection through Internal and External Audit and corporate accounting protocols for both councils.

Section 6 Human Resources

6.1 Staffing of the Monitoring Room and those responsible for the operation of the system

6.1.1 The CCTV Monitoring Room will be staffed in accordance with the OPM. Equipment associated with The System will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures.

6.1.2 Every person involved in the management and operation of the system will be personally issued with a copy of both the Code of Practice and the Procedural Manual, will be required to sign a confirmation that they fully understand the obligations and adherence to these documents places upon them and that any breach will be considered as a disciplinary offence. 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.

6.1.3 Arrangements are made for a police liaison officer to be present in the monitoring room at certain times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Operational Procedural Manual.

6.1.4 All personnel involved with the system shall receive training from time to time in respect of all legislation appropriate to their role.

6.1.5 All CCTV staff will be licensed with the Security Industry Authority for Public Space Surveillance in order to monitor and operate CCTV equipment.

6.2 Discipline

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 subject to the employing Authority discipline code. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

6.2.2 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 room and for enforcing the discipline rules. Non-compliance with this Code of Practice by any person will be considered a breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

6.3 Declaration of Confidentiality

6.3.1 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, see also Section 8 concerning access to the monitoring room by others).

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

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

7.1.2 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.

7.1.3 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.

7.1.4 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 range of the system is not surveyed by the cameras.

7.1.5 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.

7.2 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.

7.3 Secondary Control

7.3.1 No secondary control facilities are installed.

7.4 Operation of The System by the Police

7.4.1 Under extreme circumstances the Police may make a request to assume direction of The System to which this Code of Practice applies. Only requests made on the written authority of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the System owners, or designated deputy of equal standing. Any request and approval referred to above will be accepted either verbally or in writing. A verbal request or approval will be supported in writing as soon as reasonably practicable.

7.4.2 In the event of such a request being permitted, 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 Sections 6 and 7 of this Code, who will then operate under the direction of the police officer designated in the written authority.

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 Procedural Manual under a maintenance agreement.

7.5.2 The maintenance agreement will make provision for regular and periodic service checks on the equipment which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

7.5.3 The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.

7.5.4 The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

7.5.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the system.

7.5.6 It is the responsibility of the System Manager to ensure appropriate and regular contract meetings are held with the contractor to ensure compliance to the maintenance service agreements for both councils.

7.5.7 A computerised maintenance log (VTAS) will be kept and maintained in the control room by the CCTV staff, who will carry out regular daily and shift checks of all equipment and record all equipment failures, including time and date of failure recording any job or task number given by the relevant contractor, the time and date the Maintenance Contractor was notified and date when the fault was corrected. The maintenance log will correlate with other relevant system updates.

7.5.8 The maintenance log shall be fully updated by the CCTV staff, as and when maintenance contractors have visited the faulty equipment, detailing all works completed to date including if the equipment is operational and serviceable.

7.5.9 Any system failures that could cause reputational damage to both FDC or PCC, or could cause a detrimental impact on service delivery to the partnership will be raised by the CCTV staff to the CCTV shared service manager as soon as operationally possible for escalation to relevant stakeholders and system users.

7.6 Loss of computerised system

7.6.1 In the event of a loss of the computerised system (VTAS), paper logs will be substituted during the period of loss and all entries will be retrospectively included when the system is restored.

7.6.2 All incidents and other information placed on hard copy shall be entered onto the electronic systems once systems are restored and then hard copies then securely disposed of using onsite confidential waste bins.

Section 8 Access to, and Security of, Monitoring Room and Associated Equipment

8.1 Authorised Access

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

8.2 Public access

8.2.1 Public access to the monitoring and recording facility 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 OPM.

8.3 Authorised Visits

8.3.1 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 same way as that described above.

8.3.2 The CCTV shared service manager (or his/her deputy in their absence) are authorised to decide on behalf of the Councils who has access to the control room. This will normally be:

- Staff employed to operate within the control room (Including Cambridgeshire Constabulary staff) who shall all be police vetted to NPPV2 level clearance.
- Police officers authorised in a manner agreed between Cambridgeshire Constabulary and the Council: requiring to view recorded data of a particular incident, or taking written statements from a member of the CCTV staff who viewed a specific incident being investigated or collecting recording media being considered or used for evidential purposes or other specifically agreed purpose. To act as liaison officers for major events or operations.
- Other enforcement agencies by prior agreement.
- Maintenance contractors by prior arrangement.
- Accompanied visitors by prior arrangement with the CCTV shared service manager.

8.3.3 The CCTV operators will check the identity of all visitors and verify their authority to visit the CCTV shared service control room before admittance.

8.3.4 A computerised visitor's log (VTAS) will be operational and maintained in the control room by the CCTV staff who will verify their authorised visit with management, record the names of all persons entering the control room, together with times of arrival and departure and reason for the visit.

8.3.5 Visitors will be requested to read and accept the confidentiality statement on arrival conditional on permission to remain in the control room, and the operator will log them off at their departure.

8.4 Declaration of Confidentiality

8.4.1 Regardless of their status, all visitors to the CCTV monitoring room, including inspectors and auditors, will be required to book with the CCTV staff and agree to the declaration of confidentiality.

8.5 Security

8.5.1 Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the monitoring room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual will be complied with.

8.5.2 Doors leading to the control room, and other secure areas are fitted with cameras, and a door access system to restrict unauthorised entry.

8.5.3 The control room is fitted with magnetic lock security system which allows the operators to ascertain potential visitors through direct viewing of the local security cameras before allowing access.

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 the result of, technical equipment which forms part of The System, but specifically includes images recorded digitally, including digital prints.

9.1.2 Every digital recording obtained by 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 or format (e.g. paper copy, digital storage device, DVD, or any form of electronic processing and storage) of the images obtained from the system, they are treated strictly in accordance with this Code of Practice and the OPM from the moment they are received by the monitoring room until final destruction. Every movement and 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.

9.2 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 channelled through the System Manager. The System Manager will ensure the principles contained within Appendix C 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 C and this Code of Practice;
- The release or disclosure of data for 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.

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 C and the Procedural Manual.

9.2.5 It may be beneficial to make use of 'real' recorded footage for the training and education of those involved in the operation and management of CCTV systems, 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 Recordings - Provision & Quality

9.3.1 To ensure the quality of the recordings, and that recorded information will meet the criteria outlined by current Home Office guidelines, the only storage media to be used with the system are those which have been specifically provided in accordance with the OPM.

9.4 Digital Recordings – Retention

9.4.1 Digital recordings will be retained for a period of 30 days

9.4.2 Digital recordings will always be used and stored in accordance with the OPM. At the conclusion of their life within the CCTV System they will be deleted.

9.5 Digital Recording - Register

9.5.1 Each digital recording will have a unique tracking record maintained in accordance with the procedural manual, which will be retained for at least three years after recording has been deleted. The tracking record shall identify every use, and person who has viewed or had access to the recording since the initial capture of the data until its deletion.

9.6 Recording Policy

9.6.1 Subject to the equipment functioning correctly, images from every camera will be digitally recorded throughout every 24 hour period onto the digital storage system.

9.7 Images required for evidential purpose

9.7.1 In the event of a digital recording being required for evidential purposes the procedures outlined in the OPM will be strictly complied with.

9.8 Ownership of Copyright

9.8.1 All equipment located in the CCTV shared service control room and all recorded information recorded from the CCTV system and stored on any form of recording media held either internally or externally will remain the property of Peterborough City Council.

9.8.2 All equipment and data and information recorded from the CCTV system stored on any form of recording media held either internally or externally within the Fenland area will remain the property of Fenland District Council.

9.9 Security of recorded data

9.9.1 The CCTV images recorded will be securely kept on dedicated and secure servers located in ICT server rooms in Peterborough and Fenland.

9.9.2 For Peterborough, the CCTV images will be securely recorded on servers within the Sand Martin House server room, and for Fenland District Council, the CCTV images will be securely recorded on servers within the Boathouse server room.

9.9.3 Recorded data will be used only by the Council's or Cambridgeshire Constabulary or others permitted by the Council for a specific and legitimate purpose, and only then in secure conditions which is only viewable via the Councils shared service control room facility.

9.9.4 The recorded data will only be used by the Council's or by the Police or others permitted by the Council's for the following authorised purposes:

9.9.4.1 Investigation or identification of person(s) suspected of criminal or antisocial behaviour;

9.9.4.2 Production in a court of law by the Police or other law enforcement agency for evidential purposes;

9.9.4.3 Production by the Council's for lawful purposes in connection with the Council's statutory duties;

9.9.4.4 For training and promotional purposes subject to the approval by the Council's shared service CCTV manager or his/her nominee. In no circumstances will the recorded data recorded in the control room be issued, given or sold to any third party by the employees of the Council or the Police without the approval of the Council's CCTV manager or his/her nominee.

Section 10 Digital Prints

10.1 Guiding Principles

10.1.1 A digital print is a copy of an image or images which already exist on the CCTV System. Such prints are equally within the definitions of 'data' and recorded material

10.1.2 Digital prints 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 Procedural Manual.

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

10.1.4 A record will be maintained of all video print productions in accordance with the Procedural 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 records of the video prints taken will be subject to audit in common with all other records in the system.

Appendix A Key Personnel and Responsibilities

1. System Owners

Peterborough City Council
Town Hall
Bridge Street
Peterborough
PE1 1HG
Tel: 01733 747474

Fenland District Council
Fenland Hall
County Road
March
Cambridgeshire
PE15 8NQ
Tel: 01354 654321

Responsibilities:

Peterborough City Council and Fenland District Council are the joint 'owner' of the system. The Director of People and Communities (or designated person) will be the single point of reference on behalf of the PCC and the Director of Housing and Community Support (or designated person) will be the single point of reference on behalf of the FDC with responsibility to:

Ensure the provision and maintenance of all equipment forming part of the CCTV shared service system in accordance with contractual arrangements which the owners may from time to time enter into.

Maintain close liaison with the CCTV shared service manager.

Ensure the interests of the owners 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 Procedural Manual.

2. System Management

CCTV shared service manager
Fenland District Council
Fenland Hall,
March,
PE15 8NQ
Tel: 01354 654321

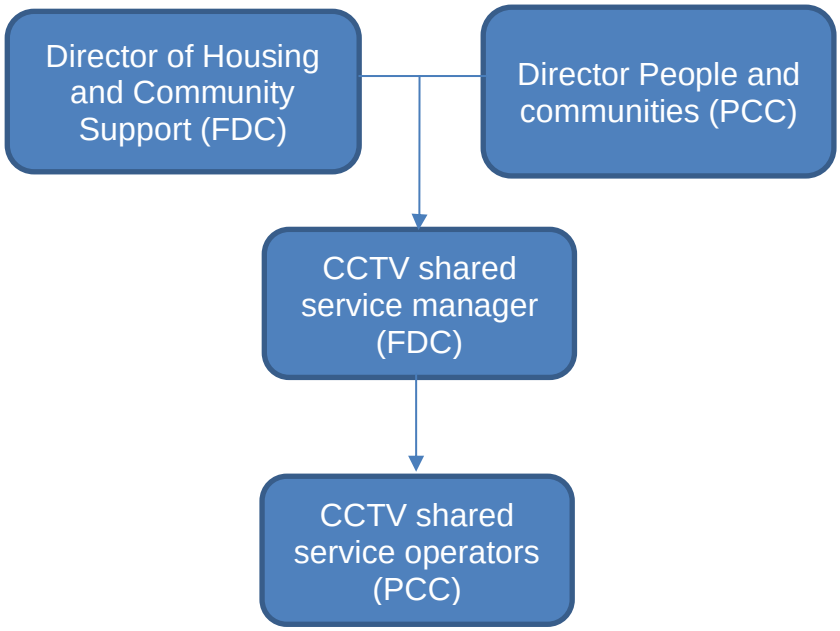
The CCTV manager is responsible for the day-to-day operational management of the system and the Single Point of Contact (SPOC) for each council.

The CCTV Manager has delegated authority for data control on behalf of the 'data controller'.

His role includes responsibility to:

- Maintain day to day management of the system and staff;
- Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with.
- Maintain direct liaison with the owners of the system.
- Maintain direct liaison with operating partners, members, customers and stakeholders

3. Management Structure for the CCTV System



Appendix B General Data Protection Regulation (GDPR) and Data Protection Act 2018

For information regarding access to personal data follow the below links to the Information Commissioners Office in relation to Subject Access Requests (SAR)

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

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

Introduction

Arguably CCTV is one of the most powerful tools to be developed during recent years to assist with 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.

Peterborough City Council, Fenland District Council and Cambridgeshire Constabulary are 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 security 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 nationally recommended standard of

The CCTV User Group has been adopted by the System owners.

1. **General Policy**

   All requests for the release of data shall be processed in accordance with the Procedure Manual. All such requests shall be channelled through the data controller although day to day responsibility may be devolved to the System Manager.

2. **Primary Request To View Data**

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

      i) Providing evidence in criminal investigations or proceedings

      ii) Providing evidence in civil proceedings or tribunals but only where directly affecting the Council.

      iii) The prevention of crime

      iv) The investigation and detection of crime (may include identification of offenders)

      v) 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:

      i) Police

      ii) Statutory authorities with powers to investigate and prosecute, (e.g. Customs and Excise; Trading Standards, etc.)

      iii) Solicitors

      iv) Plaintiffs in civil proceedings

      iii) Accused persons or defendants in criminal proceedings

iv) Other agencies, as 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:

i) Not unduly obstruct a third party investigation to verify the existence of relevant data.

ii) 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.

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

i) Be satisfied that there is no inconsistency with any data held by the police in connection with the same investigation.

ii) All such enquiries are to be processed by all parties in accordance with Schedule 2, Part 1 (5) of the 2018 Act.

Notes

(1) The release of data to the police is not be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc.

(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. In the event of a search resulting in a requirement being made for the release of data, 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).

3. **Secondary Request To View Data**

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

i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. ,General Data Protection Regulations 20186, Data Protection Act 2018, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);

ii) Any legislative requirements have been complied with, (e.g. the requirements of the General Data Protection Regulations 2016 and Data Protection Act 2018 / General Data Protection Regulations 2018).

iii) 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

iv) 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:

i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of 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.

ii) If the material is to be released under the auspices of 'public well-being, health or 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.

4. **Individual Subject Access under Data Protection legislation**

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

iii) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);

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

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

c) 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 merit.

d) 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;

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

5. 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 which 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).

a. 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.

6. Media disclosure

In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:

i) 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.

ii) 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.

iii) 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).

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

7. 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.

Appendix D Restricted Access Notice

WARNING

RESTRICTED ACCESS

AREA

Everyone, regardless of status, entering this area is required to complete an entry in the Visitors log.

Visitors are advised to note the following confidentiality clause and entry is conditional on acceptance of that clause:

Confidentiality Clause:

‘In being permitted entry to this area you acknowledge that the precise location of the CCTV monitoring room is, and should remain, confidential. You agree not to divulge any information obtained, overheard or overseen during your visit. An entry in the Visitors log is your acceptance of these terms’.

Appendix E Declaration of Confidentiality

The CCTV shared service system

I, ……....., am retained by Peterborough City Council to perform the duty of CCTV Control Room…… I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

I am fully conversant with the content of that Code of Practice and understand that all duties which I undertake in connection with the CCTV shared service must not contravene any part of the current Code of Practice, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the System or the content of The Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the CCTV System, verbally, in writing or by any other media, now or in the future, (including such time as I may no longer be retained in connection with the CCTV System).

In appending my signature to this declaration, I agree to abide by the Code of Practice at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format - now or in the future.

I further acknowledge that I have been informed and clearly understand that the communication, either verbally or in writing, to any unauthorised person(s) of any information acquired as a result of my employment with Peterborough City Council may be an offence against the Official Secrets Act of 1911, Section 2, as amended by the Official Secrets Act of 1989.

Signed: ..... Print Name: .....

Witness: ..... Position: .....

Dated this ..... day of ..... (month) 20.....

Appendix F Subject Access Request Form

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

Details relating an application for CCTV footage as a Subject Access request can be found on the Councils Website at;

https://www.peterborough.gov.uk/council/council-data/cctv/

https://www.fenland.gov.uk/cctv

Appendix G Regulation of Investigatory Powers Act Guiding Principles

Advice and Guidance for Control Room Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers Act 2000.

The Regulation of Investigatory Powers Act 2000 (RIPA), amongst other subjects, relates to surveillance by the Police and other agencies (including Local Authorities) and deals in part with the use of directed covert surveillance. 3.1 of the Covert Surveillance and Property Interference (revised Code of Practice August 2018) defines this type of surveillance as:

- It is covert but not intrusive surveillance
- It is conducted for the purposes of a specific investigation or a specific operation;
- in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

Although the System's cameras are overt if they are used in such a way that falls within the definition of Directed Surveillance they will only be used if the necessary authorities have been given.

THE CCTV SYSTEM CAMERAS WILL NOT BE USED FOR PURPOSES THAT MEET THE DEFINITION OF "INTRUSIVE SURVEILLANCE" UNLESS CORRECTLY AUTHORISED.

RIPA makes provision for directed surveillance to be conducted by a Local Authority. In such cases, the written authority to carry out directed surveillance using the CCTV System will be given at the appropriate level as directed by the Act and the authority will also follow the correct process in obtaining judicial approval. The Council's RIPA policy should be adhered to in this regard. A local authority is not permitted to undertake intrusive surveillance.

The impact for staff in the Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises using the cameras. In most cases, this will fall into sub section **c** above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The code says some hours rather than minutes.

In cases where a pre-planned incident or operation wishes to make use of CCTV for such monitoring, an authority will almost certainly be required.

Police (or any other agencies) wishing to use the CCTV shared service under the provisions of RIPA will provide to the CCTV manager details of the authorisation under which surveillance will take place as below and in line with the Councils-Cambridgeshire Police protocol:

- Data and time of the authorisation granted
- Nature of the offence under investigation
- Operation Name/Reference Number
- Data and time of any renewals/cancellation

In the case of authorities given by the Police these are usually authorised by a Superintendent or above. However, if an authority is required immediately, an Inspector may authorise the surveillance. The forms in both cases must indicate the reason and should fall within one of the following categories for directed surveillance:-

An authorisation is necessary on grounds falling within this subsection if it is necessary-

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of the United Kingdom;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

(g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

Intrusive surveillance is only permitted to be authorised where it meets the following criteria and is proportionate to what it seeks to achieve:

- In the interests of national security
- For the purpose of preventing or detecting serious crime
- In the interests of the economic well-being of the UK; or
- For the purpose of preventing or detecting an offence under S188 of the Enterprise Act 2002 (cartel offence) (Competition and Markets Authority)

There exists a Protocol between Cambridgeshire Constabulary and Local Authority CCTV Partners for the use of Public Authority CCTV systems during surveillance operations conducted by Cambridgeshire Constabulary which should be adhered to alongside the council's policy.