APPENDIX 1

WIRRAL BOROUGH COUNCIL

CODE OF PRACTICE FOR THE OPERATION OF

CLOSED CIRCUIT TELEVISION

1. INTRODUCTION

1.1 This Code of Practice is intended to apply to all systems of closed circuit television which are openly operated by the Council in Wirral.

1.2 If the cameras are used to carry out surveillance of persons in a manner calculated to ensure that they are unaware it is taking place, then the operators of the cameras will be subject to the policy and procedure published by the Council on covert surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA).

1.3 This Code sets out general principles which should govern the operation of all CCTV systems by the Council. It is supplemented by more specific codes applicable to the operation of CCTV in particular circumstances eg

1.3.1 the monitoring and enforcement of traffic and parking regulations;

1.3.2 the system jointly used by Merseyside Police to monitor behaviour by the public in public places and;

1.3.3 systems installed in vehicles to monitor and record anti-social behaviour.

2. RELEVANT LEGISLATION AND GUIDANCE

2.1 The Data Protection Act 1998

Images of persons recorded on CCTV are personal data which must be processed in accordance with the requirements of the Data Protection Act 1998 the most relevant of which are:

2.1.1 Personal data shall be processed fairly and lawfully in accordance with the conditions set out in Schedule 2 of the Act.

2.1.2 Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

2.1.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

2.1.4 Personal data shall be accurate and where necessary kept up to date.

2.1.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

2.1.6 Personal data shall be processed in accordance with the rights of data subjects under the Act (eg rights to information on personal data held; rights not to have personal data disclosed to third parties unless an exemption under the Act applies).

2.1.7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

2.2 CCTV Code of Practice Issued by the Information Commissioner

This was revised in 2008 and is still applicable. It is a guide on how CCTV systems should be operated in order to comply with the provisions of the Data Protection Act 1998.

2.3 The Human Rights Act 1998

2.3.1 Article 8 of the European Convention on Human Rights Act Fundamental Freedoms applies to public authorities. It provides that everyone has the right to respect for his or her private life. Any interference with that right must fulfil a pressing need (eg protection of the public from crime) be in accordance with the law (eg Data Protection Act 1998) and be a proportionate means of achieving a legitimate objective.

2.3.2 Members of the public are entitled to varying degrees of privacy even when they are going about their business in a public place. Their reasonable expectations of privacy must be weighed in the balance against the benefits of the CCTV system in eg deterring, detecting or preventing criminal or anti-social behaviour which interferes with the rights and freedoms of the public.

2.4 Home Office Surveillance Camera Code of Practice

This was issued by the Home Office in June 2013. It applies to CCTV systems operated by public authorities. Sections 30 and 33 of the Protection of Freedoms Act 2012 require every local authority to have due regard to its contents in carrying out its functions. It is available on the Home Office website. It should be a point of reference for all persons operating CCTV systems on behalf of the Council.

3. RESPONSIBILITY FOR COMPLIANCE WITH THIS CODE

3.1 The Chief Executive and the Strategic Directors shall ensure there is a person designated as being responsible for compliance with this Code in respect of every separate CCTV system which is being used by the Council.

3.2 The Chief Executive and the Strategic Directors shall ensure that a complete inventory is made of all the CCTV systems in use by the Council together with the persons responsible for their day to day use and maintenance and the managers responsible for compliance with this Code.

4. PURPOSES OF CCTV

4.1 Each CCTV system must have a specified purpose which is in pursuit of a legimate aim and necessary to meet an identified pressing need.

4.2 Specified purposes include;

4.2.1 Prevention and detection of crime and disorder.

4.2.2. Promotion of the safety of the public.

4.2.3 Protection of the rights and freedoms of the public and of the Council's employees, agents and contractors in the performance of their duties to the Council.

4.2.4 Monitoring of traffic signal control and detection of parking contraventions.

5. RESPECT FOR PRIVACY

5.1 Before any new CCTV system is installed or cameras added to an existing installation the Chief Executive shall ensure that those persons whose privacy is likely to be affected are consulted and the outcome of that consultation taken into account by the relevant decision maker. Such consultation shall include:

5.1.1 the purposes of the installation.

5.1.2 A description of the equipment and where it is to be sited.

5.1.3 The steps taken to mitigate any invasions of privacy.

5.1.4 The means by which those consulted shall make known their responses to the proposals.

5.1.5 A reasonable time for those consulted to respond.

5.2 Following completion of the consultation the Chief Executive shall ensure that a privacy impact assessment is carried out and recorded in writing which shall include:

5.2.1 The benefits of the installation.

5.2.2 The extent to which the equipment can technically fulfil its purposes.

5.2.3 An assessment of the extent to which the installation would adversely affect reasonable expectations of privacy of any persons and how those intrusions could be mitigated or avoided.

5.2.4 A consideration of the effectiveness of alternative less intrusive methods of achieving the objective.

5.2.5 A judgment setting out the decision maker's reasons for believing that the installation is reasonably necessary and is a proportionate means of achieving the legitimate objectives of the installation.

5.3 If reasonably practicable the processes described above should also be undertaken on or before an annual review of the continued need for any CCTV installation. Priority should be given to those installations that pose the greatest risk of intrusions into personal privacy.

5.4 CCTV systems should not be capable of recording conversations.

5.5 CCTV cameras should not be used in places where there is a high expectation of privacy eg outside public toilets or in or outside changing rooms in the Council's buildings.

6. NOTICES AND COMPLAINTS

6.1 Clear and prominent signs should be displayed warning people who are likely to be monitored that CCTV is in operation, its purpose and a telephone contact number for more information and complaints. A standard template should be designed and adopted wherever this is reasonably practicable.

6.2 Any complaints received relating to the use of the CCTV system should be investigated and determined in accordance with the Council's Complaints Procedure.

6.3 The outcome of such complaints shall be reported to the Audit and Risk Management Committee.

7. ACCESS TO RETAINED IMAGES AND THEIR STORAGE

7.1 The manager responsible for the CCTV system shall designate those persons who shall have access to retained images being only those persons who have a need to know. The images should only be viewed in a secure office to which access is restricted.

7.2 Disclosures to third parties shall only be authorised by a person designated by the relevant Strategic Director or Head of Service. Such disclosures shall be in accordance with the requirements of the Data Protection Act 1998 eg to the police for the prevention or detection of crime or to a solicitor acting on behalf of a person whose property has been damaged.

7.2.1 Such disclosures shall be recorded in writing together with their justification.

7.2.2 Each Head of Service responsible for a specific CCTV system should draw up procedures for the proper and secure disclosure to

third parties of retained images which should identify who can decide to disclose, to whom, how and in what circumstances.

7.3 Images should not be retained for longer than is necessary to fulfil the purpose for which they were obtained. This will depend upon the purposes of each installation. As a general rule images should be deleted before a month has elapsed after they were recorded.

7.3.1 Retained images should be stored in a secure setting.

7.3.2 Staff should be trained in security procedures and subject to disciplinary proceedings if they fail to comply with those procedures.

7.4 Individuals have a right to view images of themselves and be provided with a copy of the images if they make a subject access request under the Data Protection Act 1998.

7.4.1 Each Head of Service shall designate a person for handling subject access requests in respect of each CCTV installation.

7.4.2 A person making such a request must sufficiently identify himself eg by a photograph and make known the date, time and location when he believes he was captured on CCTV.

7.4.3 Images of third parties should if possible be obscured unless there are good reasons for disclosing them eg administration of justice in the case of damage to property of the person making the subject access request.

8. REVIEW AND AUDIT

8.1 There should be an annual review of each CCTV system which should include:

8.1.1 whether the equipment is capable of fulfilling its purposes and conforms to approved industry standards;

8.1.2 whether it has been properly maintained;

8.1.3 whether the requirements of this Code have been observed;

8.1.4 whether staff using the system are properly trained;

8.1.5 whether its continued use is justified having regard to the considerations in paragraph 5 above and the expense of maintenance;

8.1.6 whether it should be replaced by more suitable equipment;

8.1.7 whether any complaints have been received about its use and effectiveness.

8.2 The results of the annual review should be made available to the public either on the Council's website or on request (whichever is more appropriate).

8.3 The relevant Head of Service shall be responsible for designating those managers who should carry out the annual reviews of each installation.

8.4 The Internal Audit Section of the Council should carry out periodic audits to ensure that the requirements of this Code and of the codes specific to certain types of installations are being observed.

DATED 1st DAY OF MARCH 2014