SECURITY AND RETENTION OF PERSONAL DATA DERIVED FROM RIPA INVESTIGATIONS:

APPENDIX 5

1.Security from unauthorised access.

(a) CCTV images.

(i) The manager shall designate those persons who shall have access to retained images being only those who have a need to know i.e. those closely involved in the investigation.

(ii)The images must be secured against unauthorised interference and editing by being stored securely and labelled in Council premises to which access is restricted. Records Management could offer that facility.

(iii)The images should only be capable of being viewed in Council premises not in an employee's home.

(iv) Disclosure to 3rd parties e.g. the police should (in the absence of a court order) only be authorised by a RIPA Co-ordinator or Authorising Officer and be for the purpose of preventing or detecting crime or for the purpose of legal proceedings. Such disclosures must be recorded in writing and be capable of being justified after a data protection impact assessment has been carried out which weighs in the balance intrusions into a person's privacy against the objective of crime prevention and detection. The authorisation should stipulate the period during which the personal data may be retained before destruction.

(b)Other records of investigations.

(i) To the extent that they include personal data, such records should only be accessible to those persons who have a need to know being those closely involved in the investigation and be the minimum necessary for the purpose of detecting or preventing crime or for the conduct of legal proceedings.

(ii)Disclosures to 3rd parties should only be allowed in the circumstances set out in 1(a)(iv) above.

(iii)Copying and transmission of personal data(pathways) should be limited to what is strictly necessary for the purposes of the investigation. The manager should identify those pathways and be able to demonstrate that each one was necessary and could not have been eliminated. The more pathways there are, the greater the risk of unauthorised access. Managers should consider the advantages of storing RIPA records on Microsoft TEAMS with access restricted to those employees who are closely involved in the investigation.

(iv) Electronic files containing personal data should be password protected or encrypted and access limited to those persons who have a need to know. A display of personal data on a computer screen should only take place in a setting in which no unauthorised person is present e.g. not in an open plan office or in a room at home to which other members of the household have access or are present.

(v)Paper files containing personal data should be stored securely in locked cupboards or cabinets on Council premises and not in an employee's home or vehicle and be accessible only to those employees authorised by the RIPA co-ordinator who are closely involved in the investigation.

(vi) Staff should follow the Council's security procedures as set out in its general policies on data protection.

2.RETENTION AND DESTRUCTION.

(a) CCTV images.

(i) Images should not be retained for longer than is necessary to fulfil the purpose of preventing or detecting crime or for disclosure in legal proceedings including the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996 which requires retention of all material relevant to a criminal investigation.

(ii)Subject to the above, images of persons whose privacy has been the subject of inadvertent interference should be destroyed within a month of being recorded.

(iii)Images should be destroyed as soon as the purposes in 2(a)(i) have been achieved by making access to them impossible. This will usually be no later than one month after the end of the investigation. If there has been a prosecution, however, images should be securely retained until 6 years have elapsed since the conclusion of the case or immediately thereafter if the data subject has been acquitted and there is no prospect of an appeal. Compliance is the responsibility of the RIPA co-ordinator who should carry out and record in writing monthly reviews of the necessity of retaining CCTV images.

(b)Other records containing personal data.

(i)The above procedures should also be applied to other records of personal data save that the reviews by the RIPA co-ordinator of the need to retain personal data should be conducted at not more than 6 monthly intervals and take account of legal constraints on destruction e.g.in relation to child care and adoption records. Records of RIPA investigations should only be retained if retention would enable the welfare of the child to be better safeguarded. Personal data relating to persons outside the child's family should generally be destroyed unless it concerned an investigation into possible abuse.

(ii)The outcomes of the 6 monthly reviews should be recorded in writing and made available to the Senior Responsible Officer (the Council's Monitoring Officer or the solicitor to whom he has delegated day to day management of RIPA).

(iii)Any problems concerning the reviews should be discussed at the quarterly meetings of RIPA Co-ordinators.

C.HUGHES.

Solicitor.

22/2/21