TRAFFORD
COUNCIL

POLICY FOR THE USE AND DEPLOYMENT OF CAMERA SURVEILLANCE SYSTEMS

Contents

1.0 POLICY STATEMENT

1.1 This Policy is the framework on which the Council applies the provisions of the Protection of Freedoms Act 2012 and associated legislation which governs the use of surveillance camera systems by the Council and its agents in public places, other than the Town Centre CCTV system, which is jointly operated with Salford City Council and which is subject to a separate policy and procedure.

1.2 This Policy must be read in conjunction with the Surveillance Camera Code of Practice published by the Home Office and the guidance issued by the Biometrics and Surveillance Camera Commissioner.

1.3 This policy must be applied to all surveillance camera systems operated by the Council or by the Council's agents at all times when those systems are operated within any of the Council's buildings and external public spaces. The policy must also be applied and considered before the installation and operation of any new surveillance camera systems.

1.4 Responsibility for the implementation, enforcement and maintenance of this policy rests with officer nominated as the Single Point of Contact in conjunction with the Senior Responsible Officer.

2.0 BACKGROUND

2.1 The Protection of Freedoms Act 2012 requires "relevant authorities" which includes Trafford Council, to apply the statutory code of practice published by the Home Office in respect of Surveillance Camera systems.

2.2 A "surveillance camera system" is defined by the Protection of Freedoms Act 2012 as being closed circuit television (CCTV) systems, automatic number plate recognition systems (ANPR), any other system for storing, receiving, transmitting, processing or checking any information stored by those systems for the purpose of overt surveillance in any public place. For the avoidance of doubt it includes and is not limited to static and portable CCTV and ANPR systems, body worn cameras, in car CCTV systems and systems carried by drones.

2.3 "Overt Surveillance" means any type of surveillance that does not require authorisation under the Regulation of Investigatory Powers Act 2000 ("RIPA").

2.4 "Public place" means any place to which the public have access, whether upon payment or otherwise. This includes all of the Council's buildings and premises to which the public might be admitted by appointment or otherwise and includes car parks, community centres, libraries, schools and town halls.

2.5 "System Operator" means the person or organisation that makes the decision to deploy a surveillance camera system and/or who are responsible for defining the its purpose and/or who are responsible for the use of or processing of images or other information obtained by virtue of such a system,

2.6 "System User" means a person who may be employed or contracted by the system operator who has access to live or recorded images. Such persons must be appropriately licenced where required.

2.7 It follows that where the Council has deployed a CCTV or ANPR system in any Council owned building or other premises such as a car park, that system is a relevant surveillance system operated by the Council to which the Surveillance Camera Code of Practice and this policy applies.

2.8 Appendix B shows a register of responsible and nominated officers who have specific responsibility for the discharge of functions under this policy.

2.~~8~~9 In accordance with guidance issued by the Biometrics Camera Commissioner the officer nominated as the SPOC will carry out an audit of all the relevant surveillance systems operated by and on behalf Trafford Council at least annually and will maintain a register of those systems using the register shown at Appendix B.

3.0 DEPLOYMENT OF SURVEILLANCE CAMERA SYSTEMS

3.1 When deploying or continuing to use surveillance camera systems across its estate the Council and those administering this policy will have regard to and apply the guiding principles set out within the Surveillance Code of Practice

3.2 Where it is proposed to install or deploy a surveillance camera system an application to use that system and a data protection risk assessment must be submitted to the officer nominated as the SPOC in the forms specified for use by the Biometrics Camera Surveillance Commissioner which are reproduced at Appendix C of this document.

3.3 The SPOC may only grant an application to install or deploy a surveillance camera system where:

- The use of that system is for a specified purpose which is pursuit of a legitimate aim and necessary to meet an identified pressing need;
- They have taken into account the impact of the deployment of that system on individuals and their privacy;
- Adequate provision has been made to ensure that the use of the surveillance camera system is as transparent as possible and adequate notice will be given to members of the public of the existence of the system and the publication of an access point for access to information and complaints about the system;
- Appropriate procedures are in place for the use of the system and that the proposed users of the system are properly licenced and have been trained in its use and the applicable procedures within this policy;
- There are clear defined lines of responsibility and regulation as to the use to which the surveillance camera system may be put;
- The system is designed so as not to capture and store any more images and information than is strictly necessary for the proposed use of the surveillance camera system and that there are adequate arrangements to ensure that data is securely destroyed when no longer required;
- There are clearly defined rules as to who may have access to the images and information captured by the system and for what purposes and to whom that information may be disclosed;

- The system uses approved technology;
- There are appropriate security measures to prevent unauthorised access to the system;
- There are appropriate audit arrangements in place to ensure all legal requirements are met to the standard required by good practice and this policy;
- There is a system in place to monitor use of the system to ensure that it is used in the most effective way to support public safety and law enforcement by the appropriate processing of images and information of evidential value.
- There are arrangements in place to ensure all relevant information which relates to or facilitates to the use of the system is kept up to date.

3.4 Where the SPOC in consultation with the SRO is not satisfied that the proposal to deploy or install a surveillance camera system meets all of the regulatory requirements and good practice, they shall refuse to authorise the deployment and use of that system.

3.5 Where the operation of the surveillance camera system is to be contracted out to a contractor employed by the Council, the SPOC in consultation with SRO must consider whether there are appropriate arrangements to ensure that the Contractor can and will comply with all the requirements of the Code of Practice and ensure that all proposed users of the surveillance camera systems undertake the statutory and Council's specified training on the use of the system and meet the standards of competency specified by the Council and this policy as well as being properly licenced where required.

3.6 SPECIFIED PURPOSE AND LEGITIMATE AIM

3.6.1 The use of a surveillance camera system may only be authorised and permitted where its use is necessary for a specific purpose in relation to a legitimate aim.

3.6.2 Specified purposes and legitimate aims include:

- National security;
- Public safety;
- The economic well-being of the country;
- The prevention of crime and/or disorder;
- The protection of health or morals;
- The protection of the rights and freedoms of others;

3.6.3 In practice, most of the surveillance camera systems deployed by the Council will be for the purposes of public safety or for the prevention of crime and disorder, except where, for example, an ANPR system is deployed for the purposes of imposing and collecting fees for parking in an ANPR monitored car park.

3.6.4 In determining the specified purpose and legitimate aims of the system, the needs of the end user must be taken into account at the design stage so as to ensure that the information captured meets the requirements of the end user. For example, where a CCTV system is installed at a Council building for the purposes of detecting intruders

or those committing acts of criminal damage, consideration must be given as to whether the captured images are likely to be of a sufficient quality and accurately date and time stamped so as to be capable of being used as evidence in a subsequent prosecution.

3.6.5 It is important to ensure that the specified purpose accurately identifies the purposes to which the captured data will be put, as no captured data must be used for any other purpose other than that specified unless the purposes of the systems use have been formally amended after an appropriate consultation.

3.7 THE EFFECT ON INDIVIDUALS AND THEIR PRIVACY

3.7.1 The Human Rights Act 1998, imported various rights established by the European Convention on Human Rights into English law and imposed a statutory duty on the Council not to act in a manner which is inconsistent with those rights.

3.7.2 When considering whether to approve an application for use of a surveillance camera system the SPOC and the SRO must consider the potential impact that the use of that system may have on an individual's rights under:

- Article 8 – the right to respect for private and family life;
- Article 9 – freedom of thought, conscience and religion;
- Article 10 – freedom of assembly and association, and
- Article 14 – protection from discrimination;

3.7.3 The potential impact on a person's privacy may be enhanced where:

- The proposed deployment of surveillance camera system is in public places where persons are entitled to expect a high degree of privacy, such as public lavatories or changing room where deployment of camera surveillance system is unlikely to be a proportionate method of meeting a specific need, save in the most exceptional circumstances where there are no less intrusive means of meeting the legitimate aim;

- The proposal includes an application to combine video and audio recording – the ability to record conversations is likely to be regarded as being highly intrusive even if those conversations are taking place in public and are unlikely to be a proportionate use of a surveillance system save in the most exceptional circumstances;

- The proposal includes an application to deploy facial recognition or another use of biometric data. The use of facial recognition or other biometric data must be clearly justified to establish its proportionality and procedures must ensure that there is human intervention before any decision is made which has the capability of adversely affecting an individual.

3.7.4 Data Protection Impact Assessment

3.7.4.1 In order ensure that personal data of individuals is properly protected and the use of that data is compliant with the Data Protection Act 2018 and the General Data Protection Regulations, a data protection impact assessment must be conducted as part of the authorisation process using the template form prescribed by the Biometrics Camera Surveillance Commissioner which is set out within Appendix C.

3.7.4.2 The RIPA Monitoring Officer must only grant authorisation to deploy and install surveillance camera system after considering the data protection impact assessment and being satisfied that appropriate physical and technical arrangements are in place to ensure compliance with data protection legislation and good practice.

3.8 TRANSPARENCY

3.8.1 Good practice and statutory requirements impose a duty upon the Council to ensure that members of the public are made aware whenever they are likely to be monitored by a surveillance camera system. The Code of Practice requires surveillance camera operators to be proactive in the publication of information about the use of surveillance camera systems, save that the exact location of such systems need not be revealed where such disclosure would interfere with the legitimate aim that the use of the system is designed to meet.

3.8.2 The SPOC will ensure before granting authorisation to deploy and use a surveillance camera system that:

- There has been adequate consultation with stakeholders likely to be affected by the installation of the system to ensure that it is fit for purpose and does not improperly interfere with individuals' rights. For example: where it is proposed to install a surveillance camera system in a staffed council building for the prevention of crime and disorder it would be appropriate to consult with those employees working within that building and the police who are likely to be the appropriate prosecution organisation.

- There are adequate notices informing members of the public of the use of a surveillance system, the contact details of the operator and the person(s) to whom requests for access or complaints should be addressed.

- That information is made available to the public that sets out how they may use the Council's complaint's procedure to address concerns about the use of the surveillance camera system.

- That members of the public are informed of their right to complain to the Information Commissioner or the Investigatory Powers Tribunal as appropriate in the event that the complaint is not remedied through use of the Council's complaints procedures.

3.9 RESPONSIBILITY AND ACCOUNTABILITY

3.9.1 Before authorising the deployment and use of a surveillance camera system the SPOC and SRO must consider that there are defined governance arrangements that identify the designated individual responsible for all pre-deployment consultations, design and deployment of the surveillance camera system.

3.9.2 Where the system is to be operated by a contractor employed by the Council, the SPOC in conjunction with the SRO must ensure that the contractor's governance of the system meets the Council's minimum standards and is compatible with the Council's scheme of governance.

3.9.3 The SPOC in conjunction with the SRO will also ensure that the roles and responsibilities of the operators and users of the system are clearly defined.

3.10 CLEAR RULES AND POLICIES

3.10.1 The SPOC in conjunction with the SRO will ensure that there are clear rules and policies that relate to each surveillance camera system that is to be deployed for use and that such rules and policies define who the operator and users of the system are.

3.10.2 The SPOC will only authorise persons to act as system users where they are the holders of a Level 2 Award for Working as a CCTV Operator (Public Space Surveillance) and where they hold the appropriate licence issued by the Security Industry Authority unless they are satisfied that the role of the person concerned does not require such a licence to be held or they hold an equivalent qualification.

3.10.3 Only those persons who have received appropriate training provided by the Council in the use of the system may be appointed to undertake any role under this policy.

3.10.4 The SPOC will carry out an audit of all the relevant surveillance systems operated by and on behalf Trafford Council at least annually and will maintain a register of those systems using the register shown at Appendix B.

3.11 STORAGE AND USE OF IMAGES AND INFORMATION

3.11.1 The general principle that must be applied is that data which is captured by a surveillance camera system must not be retained for any longer than is strictly necessary for the purposes for which that data is required. Once that data is no longer required it must be securely destroyed.

3.11.2 The retention period for images and other information captured by surveillance camera system will differ depending on the reason why the data was captured and its intended use and the technical specifications of the system which is in use.

3.11.2 When authorising the deployment and use of a surveillance camera system the ~~RIPA~~ SPOC in conjunction with the SRO shall ensure that the rules that apply to that system specify the maximum period in which images and data recorded by the system shall be retained, save and except where its further retention is required for an approved purpose.

3.11.3 Where images are disclosed for the purposes of a proposed or intended prosecution, the rules shall specify that the images or data shall be retained in accordance with the rules that apply under the Criminal Procedure and Investigation Act 1986 and the Codes of Practice made under that Act, or until a decision is made to discontinue or not to proceed to prosecution.

3.12 DISCLOSURE AND ACCESS TO IMAGES AND CAPTURED DATA

3.12.1 The rules that are applicable to each camera surveillance system shall specify the purposes for which images or data may be disclosed and to whom and will specify that the disclosure of such information may only take place where authorisation has been given by the system manager Data Protection Officer, save and accept where an urgent enquiry is made the police in respect of a recent or ongoing criminal investigation where urgent disclosure is required for the purpose of the investigation or prevention of criminal activity, in which case discloser may be authorised by the scheme manager, who must declare that disclosure to the SPOC no later than the next working day after disclosure for details of the disclosure to be recorded on the central register of disclosures.

3.12.3 Any subject access request from a member of the public or representative acting on behalf of a member of the public or corporation shall be referred to the Data Protection Officer for determination.

3.12.3 Under no circumstances must any data captured by a surveillance camera system be disclosed save and accept for the purpose that data was captured, save and accept where such disclosure is required by law.

3.12.4 In the event of any doubt arising as to whether any disclosure of images or data captured by a surveillance system is required by law or is capable of being authorised under the rules:

- A system manager shall refer the matter to the SPOC who will seek the decision of the Data Protection Officer as to whether the application for disclosure should be granted or refused;

- The Data Protection Officer shall seek the advice of the SRO or the Council's Legal Services Department before the application is determined.

3.12.5 In determining whether an application for disclosure should be granted, the determining officer will give active consideration to the rights of persons other than the applicant who may be depicted or be identifiable within the images sought and:

- Where the application is made by a legal representative, seek a solicitor's undertaking that the disclosed images or data will only be used for the purpose identified in the request and will not be supplied to their client electronically to create the risk that image could be uploaded to social media or be further disclosed and that the solicitor, their servants and agents will not share the images or cause or allow them to uploaded to any form of social media, using the draft undertaking shown at Appendix D.

- Where the application is made by an application from a member of the public or corporation from whom no binding undertaking can given, give active consideration as to whether the risk of further unauthorised disclosure can be appropriately managed and in the absence of being so satisfied, refuse the application until or unless it is submitted through an authorised legal representative.

3.12.6 Where the authorised disclosure of images or data risks identifying persons who are not the subject of the application consideration must be given to pixilating their images and other identifying marks, such as car registration plates so that those other persons cannot be identified.

3.12.5 The deliberate unauthorised disclosure of images or data captured by a surveillance camera system will be treated by the Council as a matter of gross misconduct.

3.13 TECHNICAL STANDARDS AND COMPETENCE

3.13.1 When authorising the deployment and use of a camera surveillance system, the SPOC shall consider whether the system meets any required standards set domestically by the British Standards Institute, at a European level by the Comité Européen de Normalisation Électrotechnique or at a global level by the International Electrotechnical Commission

3.12 DATA AND PHYSICAL SECURITY

3.13.1 In considering whether to authorise the deployment or use of a surveillance camera system, the SPOC in conjunction with the SRO must be satisfied that there are adequate physical and electronic security arrangements to protect the system and the data captured by it from theft, improper interference of unauthorised data capture.

3.13.2 Where necessary the SPOC shall seek the specialist advice of the Council's IT specialists to ensure adequate electronic security measures are present within the designed system which provide for its ongoing maintenance.

3.14 DATABASE MANAGEMENT

3.14.1 Where the operation of the camera surveillance system is dependent on data matching with an established data base such as for example the use of ANPR data, the SPOC in conjunction with the Data Protection Officer shall ensure that the proposal and the rules regarding the operation of the system contain an effective mechanism for ensuring that the databases are regularly and effectively updated.

4.0 AUTHORISED USERS

4.1 It is a requirement of the Private Security Industry Act 2001 and the Surveillance Camera Code of Practice that a system user must be appropriately licenced by the Security Industry Authority (SIA) subject to certain exemptions for in house employees.

4.2 In order to be licenced by the SIA a person who wishes to become a system user must be of good character and have obtained appropriate training from an SIA approved training organisation leading to the award of an appropriate licence by the SIA.

4.3 The SPOC is responsible for authorising officers who are permitted to have access to camera surveillance systems operated by or on behalf of the Council. Such authorisation will specify the system or systems to which that person is authorised to have access to and record any limitations to their permitted level of access to the system

4.4 The SPOC will maintain a register of officers who authorised to operate and access camera surveillance systems operated by the Council and ensure that the register is maintained and kept up to date.

5.0 MONITORING AND REVIEW

5.1 MONITORING

5.1.1 In order to maintain effective and efficient oversight of the continued necessity for each camera surveillance system, the SPOC shall maintain a central register of camera surveillance systems which are proposed, in use or which have been discontinued for use by the Council.

5.1.2 The central register will record:

- The location of the camera surveillance system
- The type of camera surveillance system

- The operator of the camera surveillance system
- The authorised users of the camera surveillance system
- The dates upon which the system was proposed, authorised or refused, the date the system became operational, the dates or review and the date upon which operation of the system ceased

5.1.3 The central register will also include details of all requests for disclosure of information from each of the camera surveillance systems, whether that request was granted or refused, the dates upon which the continued retention of disclosed information was reviewed and the dates upon which such information was destroyed.

5.1.4 The central register shall be held electronically with access to it being granted to the Chief Executive, Senior Responsible Officer, Data Protection Officer and the SPOC

5.1.5 The SPOC must update the register on receipt of any notification they receive that data from a camera surveillance system was disclosed to the police in respect of an urgent or ongoing criminal investigation by a scheme manager.

5.1.6 The SPOC must update the register with any request they receive for access to images and data captured by the camera surveillance system and the date they applied for permission to disclose that information from the Data Protection Officer.

5.1.6 The Data Protection Officer is responsible for updating the Central Register with their decision as to whether or not to authorise the disclosure of information captured by a camera surveillance system, the date and reason for their decision.

5.2 REVIEW

5.2.1 The SPOC shall ensure that a review of the need for each camera surveillance system is conducted at least annually and that the Central Register is updated as to the result of that review. The decision as to whether the need for the system continuing to be in use shall be determined using the self-assessment matrix specified by the Biometrics Camera Surveillance Commissioner which is reproduced as a specimen form at Appendix C.

5.2.2 The SPOC shall ensure that the data base of authorised users, their qualification and the training they have undertaken is updated at least every 4 months or after any key event.

5.2.3 A “key event” will occur where there has been any breach of the rules and procedures within this policy or the surveillance camera schemes rules or where there is any change in the status of an authorised user or operator.

5.2.5 The SPOC in conjunction with the SRO shall ensure that this policy is reviewed within 28 days of any change in the relevant legislation or amendments to the Code of Practice or at least annually to ensure that the policy reflects good practice and the relevant statutory requirements.

5.3 REPORTING

5.3.4 The SRO in conjunction with the SPOC shall ensure that a report to the Accounts and Audit Committee and the Executive Committee every quarter that:

- Provides details of the camera surveillance systems which have been deployed for use across the Council’s estate;

- Any new applications to deploy camera surveillance systems since the last report together with the result of that application;
- Any camera surveillance systems which have been discontinued for use;
- The number and reasons for disclosure of information captured by camera surveillance systems;
- Any breaches of the rules and procedures associated with the use of camera surveillance systems or under this policy.

5.3.5 A template for such reporting is contained within Appendix C.

Trafford Council

August 2022

APPENDIX A – SCHEDULE OF CAMERA SURVEILLANCE SYSTEMS

MS EXCEL file held remotely

Appendix B – Key Personnel

Senior Responsible Officers

Dominique Sykes

SPOC

Adrian Fisher

CCTV Managers

Nicky Shaw

Nigel Smith

Sharon Walls

System Operators

AMEY EQUANS Trafford Council

Authorised System Users

Nicola Henry

Gerard Lennox

Suzanne Whittaker

Clare Whittle

Helen Grant

APPENDIX C – FORMS

All forms are held separately and have been made available to the SPOC, CCTV Managers and authorised users.

APPENDIX D – UNDERTAKING

UNDERTAKING AS TO THE DISCLOSURE PROVISION OF DATA FROM A CAMERA SURVEILANCE DEVICE

Name of Solicitor: SRA No:
Name of Firm:
Firms Address:
Contact No: E Mail:

I, being the above named solicitor in respect of evidence from Camera Surveillance systems provided to me by Trafford Council in respect of my request for disclosure of that information dated which has been allocated the Councils reference number:

HEREBY UNDERTAKE:

1. Not to cause or permit any further copies to be made of the disclosed material in any form whatsoever, save as is permitted by clause 4;

2. To keep the disclosed material securely in the form it was provided so as to be protected from unauthorised access by any person;

3. To use his/her best endeavours to ensure that the disclosed material is kept within their personal custody and is not distributed by any insecure electronic means, courier or sent via the postal service:

4. To release the disclosed material only to:

    a. Counsel instructed in the case
    b. any expert authorised by the court to prepare a report for use by the court
    c. any other person only with the written permission of the Data Protection Officer at Trafford Council.

5. To require any person to whom the disclosed material is released to sign a form of undertaking in the same terms as this undertaking.

6. To use his/her best endeavours to obtain the return of the tapes to his/her personal possession within 28 days of its release to any person or to ensure its certified destruction where the material was disclosed in electronic form.

7. To permit his/her client to view the disclosure only at his/her professional premises and in his/her presence and, in particular not through any electronic method of communication from which a recording of the material could be made.

8. To permit other parties to the proceedings to view the tapes in the presence of that party's legal advisor at the professional premises of one of the parties' legal advisor and, in particular not through any electronic method of communication from which a recording of the material could be made.

9. To return the tapes to Trafford Council, or arrange for the secure and confidential destruction thereof, forthwith upon his/her ceasing to be instructed in this matter and in any event on closure of the case.

10. To keep a written record of the name of any person allowed access to the disclosed material and the date of their access to it and to disclose that record to Trafford Council with three working days of a request for such disclosure.

Dated this day of 202

……..