Tameside Metropolitan Borough Councils' Code of Practice for CCTV

Updated March 2024

Tameside Metropolitan Borough

Author: Dave Smith, March 2024.

Contents

1. Introduction and Objectives

1.1 Introduction

1.1.1. A Closed Circuit Television (CCTV) System is operational within Tameside. This System, known as the Tameside CCTV System, comprises a number of cameras installed at strategic locations. The cameras are fully operational and either fixed or with pan, tilt and zoom facilities. The System is operated from a central Control Centre.

1.1.2. Monitoring of the system is undertaken by suitably trained Council personnel. The maintenance contract for cameras is provided by Synetics Security Ltd.

1.1.3. CCTV cameras have played an important part in our success in cutting both crime and the fear of crime around Tameside. It has been proved effective in both cutting and detecting crime and because of this people now feel safer when they're out and about. Tameside Council is committed to continuing to use CCTV to make the borough an even safer place.

1.1.4. Operators employed in the Tameside CCTV control room are all SIA licenced and work according to the Tameside MBC's CCTV Code of Practice (the Code) which will be reviewed annually. The Code should be read in conjunction with the Tameside Operational Procedures Manual.

1.2 Definitions

1.2.1 For the purposes of this Code of Practice, the **'owner'** of the Tameside CCTV System is Tameside Metropolitan Borough Council (TMBC).

1.2.2 For the purposes of the UK Data Protection Act 2018 and the General Data Protection Regulations 2018 the **'data controller'** is TMBC

1.2.3 For the purposes of this Code of Practice, the '**Tameside CCTV System'**: means the system operated by TMBC.

1.2.4 For the purposes of this Code of Practice, the **'System Manager'**: means TMBC's Integrated Neighbourhood Services Manager.

1.2.5 Details of key personnel, their responsibilities and contact points are shown at **appendix 1** to this Code.

1.3 Partnership Statement In Respect of the Human Rights Act 1998

1.3.1 Tameside Metropolitan Borough Council 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. The Council considers that the use of CCTV in Tameside is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

1.3.2 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. The Local Authority and Police also consider it a necessary initiative towards their duty under the Crime and Disorder Act 1998.

1.3.3 The Tameside CCTV System shall be operated with respect for all individuals, recognizing 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.

1.3.4 Further, the Tameside CCTV System shall be operated in such a way as to avoid infringement of individual privacy.

1.3.5 The Council recognises 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 or public safety;
- The economic wellbeing 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.

1.3.6 The Code of Practice and observance of the Operational Procedures contained in the manual shall ensure that evidence is secured, retained and made available as required so that there is absolute respect for everyone's right to a free trial.

1.4 Objectives of the System

1.4.1 The objectives of the Tameside CCTV System as determined by the Data Controller and which form the lawful basis for the processing of data are:

- To Assist in the detection, prevention and deterrence of crime and disorder in the area this will include:
  - Countering terrorism;
  - Helping to identify, apprehend and prosecute offenders;
  - Provide the police, other agencies and the Borough Council with evidence to take criminal and civil action in the courts;
  - To help reduce the fear of crime and provide reassurance to the public;
  - To increase public safety for those people who live, work, trade and visit Tameside
  - To assist in the overall management of the public space;
  - To help deter and detect acts of anti-social behaviour;
  - To enhance community safety, assist in developing the economic wellbeing of the Tameside area and encourage greater use of the town centres;
  - To assist in the enforcement and regulatory functions within the Tameside area

- To assist in Traffic Management;
- To assist in monitoring any Emergency Planning Operations;
- To assist members of the public, businesses or professional individuals with their requests for the appropriate or permitted information pertaining to incidents that may occur within the Tameside area;
- To provide a tool by which the permitted or authorised 'users' may better and more efficiently undertake their departmental, business unit or contractual responsibilities for TMBC.

1.4.2 Within this broad outline, the Data Controller may draw up specific key objectives (which will be reviewed annually) based on local concerns.

1.5 Operational Guidance

1.5.1 This Code of Practice (hereafter referred to as 'the Code') is supplemented by a separate 'Operational Guidance', which offers instructions on all aspects of the day-to-day operation of the Tameside CCTV System. To ensure the purpose and principles (see Section 2) of the Tameside CCTV System are realised, the Operational Guidance is based and expands upon the contents of this Code of Practice.

2. Statement of Purpose and Principles

2.1 Purpose

2.1.1 The purpose of this Code is to state how the owner and the System Manager intend to use the Tameside CCTV System to meet the objectives and principles outlined in Section 1.

2.2 General Principles of Operation

2.2.1 The Tameside CCTV 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 Tameside CCTV System will also recognise the need for formal authorisation of surveillance as required by the Regulation of Investigatory Powers Act 2000, in particular Part 2 of the Act, the Police force policy and the Office of Surveillance Commissioners Procedures and Guidance issued in December 2014.

2.2.3 The Tameside CCTV System will be operated in accordance with the UK Data Protection Act 2018 and the General Data Protection Regulations 2018 at all times.

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

2.2.5 The Tameside CCTV System will be operated with due regard to a general 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 Tameside CCTV System will be safeguarded by ensuring the security and integrity of operational procedures.

2.2.7 Throughout this Code it is intended, as far as reasonably possible, to balance the objectives of the Tameside 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 Tameside CCTV System is not only accountable, but is seen to be accountable.

2.2.8 Participation in the Tameside CCTV 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 it.

2.3 Copyright

2.3.1 Copyright and ownership of all material recorded by virtue of the Tameside CCTV System will remain with the Data Controller.

2.4 Cameras and Area Coverage

2.4.1 This Code refers to areas of operation of the Tameside CCTV System.

2.4.2 All cameras within the Tameside CCTV System will be positioned within an area suitably signed to alert of their presence.

2.5 Monitoring and Recording Facilities

2.5.1 All cameras are connected to a Control Centre. All images captured by the Tameside CCTV System are recorded throughout every 24 hour period by the Control Centre designated for that purpose. Monitoring hours may be subject to review and change.

2.6 Human Resources

2.6.1 Unauthorised persons will not have access without an authorised member of staff being present.

2.6.2 The Control Centre shall be staffed by trained operators in accordance with the requirements of the Private Security Industry Act 2001.

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

2.7 Processing and Handling of Recorded Material

2.7.1 No recorded material will be released from the Control Centre unless it is in accordance with this Code. Please see paragraph 9 for further details.

2.8 Operators Instructions

2.8.1 The Control Centre has its own Operational Guidelines, which comply with this Code.

2.9 Changes to the Code

2.9.1 Any major changes to the Code, will take place only after consultation with key stakeholders and following approval by the Council under its Constitution.

2.9.2 A minor change, (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the System Manager and the Owner of the System.

Notes:

- The installation of a CCTV camera is considered to be overt unless it is installed in a manner whereby its presence is deliberately intended to be concealed from the view of any person likely to be within the field of view of that camera.
- Cameras, which may be placed in domes or covered to reduce the likelihood of assessing their field of view, or to protect them from weather or damage, would not be regarded as covert provided that appropriate signs indicating the use of such cameras are displayed in the vicinity.
- TMBC will not utilise 'dummy' cameras. The greatest deterrent value of a CCTV System is its power to produce evidential material and, in doing so, to reassure those it is intended to protect.

Privacy & Data Protection

3.1 Public Concern

3.1.1 Although the majority of the public at large may have become accustomed to 'being watched', 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.

3.1.2 '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;

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

3.1.3 All personal data obtained by virtue of the Tameside CCTV System, shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives. In processing personal data a person's right to respect for his or her private and family life and their home will be respected.

3.1.4 The processing, storage and security of the data will be strictly in accordance with the requirements of the UK Data Protection Act 2018 and the General Data Protection Regulations 2018 and additional locally agreed procedures.

3.1.5 Cameras will not be used to look into private residential property, unless pursuing a suspect and this is considered to be in the interests of the private residents. Operators will be specifically trained in privacy issues. Where possible, privacy zones will be programmed into the system to obscure the view of private property and to prevent unintentional collateral intrusive surveillance.

3.2 Data Protection Legislation

3.2.1 The operation of the Tameside CCTV 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 Tameside CCTV System is Tameside Metropolitan Borough Council and day to day responsibility for the data will be devolved to the System Manager.

3.2.3 All data will be processed in accordance with the principles of the General Data Protection Regulations 2018 which are in summarised form:

5 General Data Protection Regulations principles relating to processing of personal data

1. Personal data shall be:

   A. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
   B. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
   C. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
   D. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
   E. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
   F. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

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 Tameside CCTV System will be directed in the first instance to make an application via the Subject Access Request procedure.

3.3.2 If the request cannot be complied with without identifying another individual, permission from that individual must be obtained unless it is reasonable in all the circumstances to comply with the request without the consent of that individual.

3.3.3 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located.

3.4 Exemptions to the Provision of Information

3.4.1 The provision of data may be exempt in certain circumstances, this includes:

Personal data processed for any of the following purposes:

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

Requests for personal data are exempt from the subject access provisions in any case where the application of those provisions to the data would be likely to prejudice the matters referred to above.

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

3.5 Criminal Procedure and Investigations Act 1996

3.5.1 The Criminal Procedure and Investigations Act 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the presentation of its own case, (known as unused material). An explanatory summary of the provisions of the Act is contained within the Operational Guidance, but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by the UK Data Protection Act 2018 and the General Data Protection Regulations 2018, (known as subject access).

4 Accountability and Public Information

4.1 The Public

4.1.1 For reasons of security and confidentiality, access to the Control Centre is restricted in accordance with this Code. However, in the interest of openness and accountability, anyone with legitimate reasons wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with the System Manager.

4.1.2 Cameras will not be used to look into private residential property.

4.1.3 A member of the public wishing to register a complaint with regard to any aspect of the Tameside CCTV System may do so by contacting:

Write to:
PO Box 317
Ashton-under-Lyne
OL6 0GS

E-mail to informationanddata@tameside.gov.uk

4.1.4 All complaints shall be dealt with in accordance with the Tameside MBC complaints procedure. Any performance issues identified will be considered under TMBC's disciplinary procedures to which all employees, including CCTV personnel are subject.

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

4.2 System Manager

4.2.1 The System Manager will have day-to-day responsibility for the Tameside CCTV System as a whole. The Tameside CCTV System will be subject to the usual Local Government audit arrangements.

4.3 Public Information

4.3.1 A copy of this Code shall be published on TMBC's web site, and a copy will be made available to anyone on request.

4.3.2 Signs have been placed in the locality of the cameras and at main entrance points to the relevant areas. The signs indicate:

- The presence of CCTV monitoring;
- The purpose for the scheme
- The 'ownership' of the Tameside CCTV System;
- Contact telephone number for the Tameside CCTV System.

5. Assessment of the System and Code of Practice

5.1 Monitoring

5.1.1 The System Manager will accept day-to-day responsibility for the monitoring and operation of the Tameside CCTV System and the implementation of this Code.

5.1.2 The System Manager shall also be responsible for maintaining full management information as to the incidents dealt with by the Control Centre, for use in the management of the Tameside CCTV System and in future evaluations.

5.2 Audit

5.2.1 There will be regular audits of the operation of the Tameside CCTV System and the compliance with this Code. Audits, which may be in the form of irregular spot checks, will include examination of the Control Centre records, media histories and the content of recorded material.

6 Human Resources

6.1 Staffing of the Monitoring Room

6.1.1 The Control Centre will be staffed in accordance with the Operational Guidance. Equipment associated with the Tameside CCTV System will only be operated by authorised personnel who will have been properly trained in its use and all Operational Guidance.

6.1.2 Every person involved in the management and operation of the Tameside CCTV System will be personally issued with a copy of both this Code and the Operational Guidance, and will be required to sign a confirmation that they fully understand the obligations 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 have been made for police officers to be present in the Control Centre at certain times, subject to locally agreed protocols. Any such person must also be conversant with this Code and associated Operational Guidance.

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

6.2 Discipline

6.2.1 The System Manager will accept primary responsibility for ensuring there is no breach of security and that this Code is complied with. The System Manager has day-to-day responsibility for the management of the room and for enforcing the discipline rules. Non-compliance with this Code by any person will be considered a severe 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 and who has any involvement with the Tameside CCTV System to which they refer, will be required to sign a declaration of confidentiality. This is done so by all staff and visitors upon every entry into the Control Centre.

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 Cameras will not be used to look into private residential property, unless pursuing a suspect and this is considered to be in the interests of the public. (See Section 4).

7.1.4 Camera operators will be mindful of exercising prejudices, which may lead to complaints of the Tameside CCTV 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 Tameside CCTV 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 In the event of a problem with the Primary Control Centre room secondary reviewing facilities can be accessed using the Synergy “follow me” function. 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 control at all times and no access to the movement of cameras is given to this facility.

7.4 Operation of The System by the Police

7.4.1 The police may make a request to assume direction of the Tameside CCTV System to which this Code applies. Only requests made on the written authority of a police officer of Superintendent rank or above will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the owners, or designated deputy of equal standing.

7.4.2 In the event of such a request being permitted, the Control Centre 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.

7.4.3 In very extreme circumstances a request may be made for the police to take total control of the Tameside CCTV System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the Owners.

7.4.4 Any such request must be made to the System Manager in the first instance, who will consult personally with the most senior officer of the Owners (or designated deputy). A request for total exclusive control must be made in writing by a police officer of the rank of Assistant Chief Constable or above.

7.5 Maintenance of the System

7.5.1 To ensure compliance with the Information Commissioners Code of Practice and the Biometrics and Surveillance Camera Commissioners guidance - being all images recorded continue to be of appropriate evidential quality the Tameside CCTV System shall be maintained under a maintenance agreement.

7.5.2 The maintenance agreement will make provision for quarterly 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 It is the responsibility of the System Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

8 Access to and Security of Monitoring Room and Associated Equipment

8.1 Authorised use of the CCTV System

8.1.1 Only trained and authorised personnel will operate any of the equipment located within the Control Centre, (or equipment associated with the Tameside 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 Operational Guidance.

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.

8.4 Declaration of Confidentiality

8.4.1 Regardless of their status, all visitors to the Control Centre, including inspectors and auditors, will be required to sign the visitors log and a 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 Control Centre having to be evacuated for safety or security reasons, the provisions of the Operational Guidance will be complied with.

8.5.2 The Control Centre will at all times be secured by ‘Magnetic-Locks’ operated by the CCTV operator.

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 Tameside CCTV System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.

9.1.2 Every video or digital recording obtained by using the Tameside CCTV System has the potential of containing material that may need to be admitted in evidence at some point during the period of its retention.

9.1.3 Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of the Tameside CCTV 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, video tape, CD, DVD, or any form of electronic processing and storage) of the images obtained from the Tameside CCTV System, they are treated strictly in accordance with this Code from the moment they are received by the Control Centre until final destruction. Every movement and usage will be meticulously recorded.

9.1.5 Clear operational procedures are followed when retrieving video and processing images from the CCTV system by CCTV Staff using the guidelines set out in the Home Office Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0.

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

9.1.7 Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment or otherwise made available for any use incompatible with this Code.

9.1.8 Information will be made available for traffic and transport monitoring, management, enforcement and information purposes

9.2 National Standard for the Release of Data to a Third Party

9.2.1 Every request for the release of personal data generated by the Tameside CCTV System will be channelled through the System Manager or his/her representatives. The System Manager will ensure the principles contained within Appendix 3 to this Code 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;
- Access to recorded material will only take place in accordance with the standards outlined in Appendix 3 and this Code;
- 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 A.3, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. This can only be done with the agreement of the System Manager.

9.2.4 If material is to be shown to witnesses, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix 3.

9.2.5 It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of the Tameside CCTV System, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of the Tameside CCTV System will only be used for such bona fide training and education purposes.

9.2.6 Recorded material may be used for research purposes whereby there is a data sharing agreement in place with a university.

9.3 Recorded Material – Retention

9.3.1 Recorded material will be retained for as long as is operationally necessary and in any case up to a period of 31 days. All digital recording will be set to overwrite automatically.

9.4 Record of Recorded Material

9.4.1 Each operator has a specific user name and password for the Tameside CCTV System which maintains an audit record of all recorded material, each occasion on which that material has been accessed, retrieved, recorded or viewed.

9.5 Recording Policy

9.5.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period in time-lapse mode, onto digital tape or digital hard drive.

9.5.2 Images from the CCTV Operator's main monitor will be recorded in real time, and the operators will have discretion as to which cameras are selected on the main monitor. These will usually be the incident that has the highest priority at the time.

9.6 Release of Recorded Material

9.6.1 If recorded material is released in accordance with this code, a record must be kept which identifies the basis for that release, and to whom. Records will be retained for at least two years.

9.7 Prints of Recorded Material

9.7.1 Prints will be treated in the same way as other recorded information identified above. They will not be released outside the Control Centre except as permitted by this code, and any release will be recorded.

9.7.2 Where prints, which contain personal data, are taken for use within the Control Centre, they should not be kept for longer than can be reasonably justified, and should be regularly reviewed. Prints that are no longer required will be securely destroyed.

APPENDIX 1 - Key Personnel and Responsibilities

System Owners

Tameside Metropolitan Borough Council
Tameside One
Market Place
Ashton-under-Lyne
OL6 0GA

Responsibilities:

Tameside Metropolitan Borough Council is the 'owner' of the system. The System Manager will be the single point of reference on behalf of the owners. His/her role will include a responsibility to:

- Ensure the provision and maintenance of all equipment forming part of the System in accordance with contractual arrangements, which the owners may from time to time enter into.
- Maintain close liaison with the System Manager.
- Ensure the interests of the operating partners and other organisations are upheld in accordance with the terms of this Code of Practice.
- Agree to any proposed alterations and additions to the system, this Code of Practice and / or the Operational Guidance.

Operational Management

System Manager

Partnership Manager
Community Safety
Tameside Metropolitan Borough Council
Tameside One
Market Place
Ashton-under-Lyne
OL6 0GA

- The System Manager is the 'manager' of the Tameside CCTV System
- He/she has authority for day-to-day management on behalf of the 'data controller'.
- To maintain day to day management of the Tameside CCTV System and staff;
- To accept overall responsibility for the Tameside CCTV System and for ensuring that this Code of Practice is complied with;
- To maintain direct liaison between the System Owner and operating partners.

APPENDIX 2 - Extracts from UK Data Protection Act 2018

The full General Data Protection Regulations 2018 (GDPR) can be access via this link:

https://gdpr-info.eu/

Art. 5 GDPR Principles relating to processing of personal data

3. Personal data shall be:

   G. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
   H. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
   I. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
   J. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
   K. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
   L. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

The GDPR sets out seven principles for the lawful processing of personal data. Processing includes the collection, organisation, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure or destruction of personal data. Broadly, the seven principles are :

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

1 Lawful, fair and transparent processing

This principle emphasises transparency on how and why data is collected. You must have identified legal grounds under the GDPR (known as a “lawful basis” – of which there are six) for collecting and using personal data. You must ensure you are not in breach of other laws while processing. Personal data must be used in a way that is fair to the individuals – and you must be honest and open with individuals as to the use of their data.

2 Purpose limitation

This principle emphasises the need for organisations to be clear about what your purposes for processing are from the start. You must be clear about what your purposes for processing are from the start and these must be recorded as part of your documentation obligations (the accountability principle). You can no longer collect irrelevant information – it must serve a purpose. If a new purpose of processing arises, this data can only be used if it is compatible with the original, you gain consent, or if you have a clear basis in law.

3 Data minimisation

This principle emphasises the need for organisations to minimise the data they collect
All data collected must serve a purpose. This principle is designed to address today’s digital landscape where nearly every conceivable piece of data can be collected in some way. To comply with the GDPR, organisations must only store the minimum data required.
You must ensure the personal data you are processing is:

- Adequate – sufficient to properly fulfil your stated purpose
- Relevant – has a link / is relevant to that purpose
- Limited to what is necessary – you do not hold more than you need to for that purpose.

4 Accurate and up-to-date processing

This principle requires controllers to ensure the information they hold is accurate and up-to-date and remains so. It is only lawful to use if it remains accurate and relevant. You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading in any way. If you discover that the personal data is incorrect or misleading, you must take all reasonable steps to correct or erase it as soon as possible. This principle is designed to ensure stored data is accurate and useful to the organisation using it.

5 Storage limitation

This principle emphasises the need for organisations not to keep data longer than there is a need.

Article 5(1)(e) states personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Even if you collect and use it lawfully, you cannot keep it for longer than you actually need it.
The GDPR does not set specific time limits for different types of data – this is up to you, but the retention periods you specify for the different data types should be reflected in your data retention policy.

6 Integrity and confidentiality (security)

This principle protects the integrity, privacy and confidentiality of data by placing specific obligations on organisations to secure it. Organisations who collect and process data are to be solely responsible for the security of that data, and those security measures must be wholly proportionate to the data type. To be compliant, organisations must enforce a strict data security policy that protects data from all threats.

7 Accountability principle

This principle makes the organisation responsible for complying with the GDPR and demonstrates that you are compliant – you must take responsibility for the processing activities you carry out. To ensure on-going compliance, every step of your GDPR strategy must be auditable through the use of policies and procedures. In the event of an investigation, you can prove that the proper actions have been taken, or, at the very least, you can show considerations were made. These obligations are on-going and must be reviewed at appropriate intervals.

APPENDIX 3 - National Standard for the release of data to third parties

A.3.1 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.

Tameside MBC is committed to the belief that everyone has the right to respect for his or her private and family life. 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.

The ICO's Code of Practice on Data Sharing does not prescribe national standards but outlines the framework under which disclosure can be made. After considerable research and consultation, the nationally recommended standard of The CCTV User Group has been adopted by the System owners.

A.3.2 General Policy

All requests for the release of data shall be processed in accordance with the Operational Guidance. All such requests shall be channelled through the data controller or his nominated representative.

A.3.3 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 proceedings;
   ii) Providing evidence in civil proceedings or tribunals
   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 prosecute, (e.g. Customs and Excise;
   iii) Trading Standards, etc.)
   iv) Solicitors
   v) Claimants in civil proceedings
   vi) Accused persons or defendants in criminal proceedings
   vii) Other agencies, (as agreed by the Data Controller and notified to the Information Commissioner) 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) Where requests fall outside the terms of disclosure and Subject Access legislation, the data controller, or nominated representative, shall:

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

Notes

1) 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. 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.

2) 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.

3) 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.

4) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. Time and date of an incident should be given to the nearest half an hour.

A.3.4 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. UK 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 UK Data Protection Act 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’ (1).

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 (2).

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.

Notes:

1) 'Disclosure in the public interest' could include the disclosure of personal data that:

   i) provides specific information which would be of value or of interest to the public well being
   iii) identifies a public health or safety issue
   iv) leads to the prevention of crime

2) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request, (see III above).

A.3.5 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) A specified fee is paid for each individual search;
   iii) The data controller is supplied with sufficient information to satisfy him or herself as to the identity of the person making the request;
   v) 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 the council considers that within one hour of accuracy would be a reasonable requirement);
   vi) The person making the request is only shown information relevant to that particular search and which contains personal data of her or himself 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). Under these circumstances an additional fee may be payable.

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

e) A copy of the Council's 'Subject Access Request Form' along with the Council's guidance, is available at: https://www.tameside.gov.uk/dataprotection/access

A.3.6 Process of Disclosure:

a) Verify the accuracy of the request.
b) Replay the data to the requestee only, (or responsible person acting on behalf of the person making the request).
c) The viewing should take place in a separate room and not in the control or monitoring area. Only data that is specific to the search request shall be shown.
d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

A.3.7 Media disclosure

a) 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, and indemnifies the partnership against any breaches of the legislation.
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.
iv) 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).
v) The release form shall be considered a contract and signed by both parties.

APPENDIX 4 - Tameside's 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 accompanied by your signature in the Visitors log is your acceptance of these terms'.

APPENDIX 5 - Declaration of Confidentiality

The Tameside CCTV System

CCTV CODE OF PRACTICE DECLARATION

This is to certify that I have read and understood the requirements of the attached Code of Practice in respect of the monitoring and recording of images from the system and that I shall abide by its requirements at all times during my employment within the monitoring room having particular regard to the human rights of individuals and the protection of personal data.

I further certify that I shall ensure that any personal data, intelligence or evidence which I have had access to during my employment shall remain strictly confidential during and after my employment.

Signed……..

Name……..

Address……

…….

……..

Date……...

APPENDIX 6 - Regulation of Investigatory Powers – Guiding Principals

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

The Regulation of Investigatory Powers Act 2000 relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26(2) of the Act sets out what is Directed Surveillance. It defines this type of surveillance as:

*Subject to subsection (6), surveillance is directed for the purposes of this Part if it is **covert** but **not intrusive** and is undertaken:*

(a) for the purposes of a specific investigation or a specific operation;
(b) 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
(c) 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

The impact for staff in the Control Centre, 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.

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

RIPA requests are authorised by a Superintendent or above. The forms must indicate the reason and should fall within one of the following categories:

28(3) 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.

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then in writing by way of the forms. Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising.

APPENDIX 7 - Subject Access Request Application Form

Tameside MBC is a Data Controller registered with offices of the Information Commissioner and the Biometrics and Surveillance Camera Commissioner. This to ensure that any data we gather about you will be processed, stored and distributed lawfully and to give you the confidence that we will respect your right to privacy at all times.

National Standard for the Release of Data to a Third Party

Every request for the release of personal data generated by the Tameside CCTV System will be channelled through the System Manager or his/her representative. The System Manager will ensure the principles contained within Tameside CCTV Code of Practice are followed at all times.

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 the Tameside CCTV Code of Practice (The Code);
- Access to recorded material will only take place in accordance with the standards outlined in Appendix 3 of The Code;
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Data released to a third party remains the property of Tameside MBC and by signing the declaration you agree to abide by the conditions set out below.

- You will not share, publish or otherwise distribute this data.
- You will not use this data for entertainment purposes.
- You will not post this data on social media.

If you have been involved in an accident or been a victim of crime the police have the right to access stored data without the need for you to fill in this form.

Similarly, your insurance company or solicitor has the right to request data on your behalf if you have been involved in an incident. In this instance your representative will still need to provide evidence of who you are and you must supply them with a covering letter providing permission for them access your data.

Subject Access Request Application Form

Completing a “Subject Access Request” form is how you can apply for access to information held on the Tameside CCTV System.

Please note that recorded data is only stored for 31 days and requests for information that fall outside that period cannot be considered.

This guide will help you through the process of accessing data the council may have gathered about you using the Tameside CCTV system.

Your Rights

Subject to certain exemptions you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form, except where the supply of such a copy is not possible, would involve disproportionate effort, or if you agree otherwise. Tameside Metropolitan Borough Council will only give that information if it is satisfied as to your identity.

If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless:

- The other individual has consented to the disclosure of information.
- It is reasonable in all circumstances to comply with the request without the consent of the other individual(s).

The Council’s Rights

Tameside Metropolitan Borough Council may deny access to information where the General Data Protection Regulation Act allows. The main exemptions in relation to information held on the Tameside CCTV system are:

- Where the information may be held for the prevention and detection of crime or the apprehension and prosecution of offenders
- Giving you the information may be likely to prejudice any of these purposes.

Making a request:

You can make a Subject Access Request by:

Writing to the Council at
PO Box 317
Ashton-under-Lyne
OL6 0GS

E-mail to informationanddata@tameside.gov.uk

Handing your request in to any of the Council's offices, libraries and customer services centres. Contact details and locations for these can be found at:
www.tameside.gov.uk/servicecharter/custserv or www.tameside.gov.uk/libraries

Filling in and returning this Subject Access Request form.

If any of the information required in the form has already been supplied, i.e. in a written or emailed request, there is no need to complete that section of the form.

The Application Form.

This application form has been designed to be completed easily and within just a few minutes once you have read through the covering information.

Any concerns or difficulties you experience should be reported to:

The Tameside CCTV System Manager, Dave Smith, and addressed to Dave.Smith2@tameside.gov.uk

All relevant sections of the forms must be completed and failure to do so may delay your application.
As soon as you have supplied sufficient information, the Council will gather the data you require and respond to your request as soon as possible and no later than one calendar month.

Section 1 asks you to give information about yourself that will help the Council to confirm your identity. The Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full face photograph of you.

Section 3 asks you to confirm that you want a copy of the information.

Section 4 asks you to sign the declaration.

Section 5 is about finding the information you are requesting.

Please note that any data supplied must be collected in person and must be signed for.

If you have any queries regarding this form or your application, please contact CCTV@Tameside.gov.uk

What if I'm not satisfied with the Council's response?

If you are not satisfied with the response you may complain by email to: informationanddata@tameside.gov.uk.

Or in writing to:
Information and Data Team,
Tameside One,
PO BOX 317,
Ashton under Lyne, OL6 0GS.

You may also complain at any time to the Independent Information Commissioner about the information Tameside Metropolitan Borough Council or any other organisation is processing about you. If you contact the Information Commissioner first, it is likely your complaint will be passed to the Council to give us an opportunity to respond. The Information Commissioner cannot award any compensation to you where there has been a breach of the General Data Protection Regulations Act.

He can, however, provide you with further information to enable you to enforce your rights or he can consider your complaint and make an assessment.

In some cases where the Information Commissioner believes the Data Protection Act has not been complied with he will issue an enforcement notice to the Data Controller. Failure to comply with that notice is a criminal offence.

The Information Commissioner will not take enforcement action in every case. The Information Commissioner may be contacted at:

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
Fax: 01625 524510

Website: Information Commissioner's Office (ICO)

Further information about your rights is available from the ICO website here: For the public | ICO

SUBJECT ACCESS REQUEST APPLICATION FORM

SECTION 1: About Yourself

The information requested below is to help the Council (a) satisfy itself as to your identity and (b) find any data held about you. **PLEASE USE BLOCK CAPITAL LETTERS.**

Title (tick box as appropriate)	**Mr** ☐ **Mrs** ☐ **Miss** ☐ **Ms**☐ **Other:**
Surname / family name	
First Name(s)	
Maiden name / former names	
Sex (tick box as appropriate)	**Male** ☐ **Female** ☐
Height	
Date of Birth (DD/MM/YYYY)	
Place of Birth (Town and County)	
Your Current Home Address or email address (to which you wish us to reply)	
Postcode	
Telephone Number	

If you have lived at the above address for less than 10 years, please give your previous address(s) for the period:

Previous Address 1		
Postcode		
Dates of Occupancy (MM/YYYY)	**From:**	**To:**
Previous Address 2		
Postcode		
Dates of Occupancy (MM/YYYY)	**From:**	**To:**

SECTION 2: Proof of Identity

To help establish your identity your application must be accompanied by **TWO** official documents that between them clearly show your **name, date of birth and current address**.

For example:

- Birth / adoption certificate
- Driving licence
- Medical card
- Passport
- Other official document that shows your name and address.

Also a recent **full face photograph of yourself** is required.

Failure to provide this proof of identity will delay your application.

SECTION 3: Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form.

Please confirm that you will sign for and collect the released information.

I am willing to sign for and collect a permanent copy	☐

SECTION 4: Declaration

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by	
Date (DD/MM/YYYY)	

Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.

SECTION 5: Finding the information you are requesting

If the information you have requested refers to a specific offence, incident, vehicle, property or another specific type of information, please complete this section.

In order to ensure your request can be complied with please provide as accurate a time as possible for the incident you are enquiring about, within half an hour of the actual incident.

For example, if you report the incident as occurring at 6:30am a time frame of 6am until 7am will be checked.

Were you: (tick box below as appropriate)

A person reporting an offence or incident	☐
A witness to an offence or incident	☐
A victim of an offence	☐
A person accused or convicted of an offence	☐
Other- please explain	
Date of Incident (DD/MM/YYYY)	
Time of Incident	
Location of Incident	
Brief details of Incident	

Before returning this form make sure you have:

- Completed ALL relevant Sections in this form.
- Enclosed TWO identification documents.
- Enclosed a recent full face photograph of yourself.
- Signed and dated the form.

Further Information:

These notes are only a guide. The law is set out in the General Data Protection Regulations Act, obtainable from The Stationery Office. Further information and advice may be obtained from:

The Information Commissioner,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire SK9 5AF.
Telephone: 0303 123 1113
Fax: 01625 524510

Please note that this application for access to information must be made direct to **Tameside Metropolitan Borough Council** and **NOT** to the Information Commissioner.

The completed form and the required identification documents should be returned to:

PO Box 317
Ashton-under-Lyne
OL6 0GS

Or by e-mail: informationanddata@tameside.gov.uk

Please note that any data supplied must be collected in person and must be signed for.

OFFICIAL USE ONLY

Please complete ALL of this Section.

Application checked and eligible?	
Identification documents checked?	
Date Application Received (DD/MM/YYYY)	
Details of 2 Documents (See Section 2)	
Documents Returned?	Yes ☐ No ☐
If the SAR form has not been completed have you ensured that the customer is aware of the terms and conditions of this agreement.	Yes ☐ No ☐

Member of Staff completing this Section:

Name	
Job title	
Signature	
Date (DD/MM/YYYY)	