Blaenau Gwent County Borough Council

Public Space CCTV System

Code of Practice

<Final Working Draft>

To be considered for review: March 2022

Contents

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect of Blaenau Gwent County Borough Council's Public Space Closed Circuit Television System and, as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of this System.

Signed for and on behalf of Blaenau Gwent County Borough Council, the 'System Owner'

Signature: .....…….....

Name: ……

Position held: Chief Finance Officer

Section 1 Introduction & Objectives

1.1 Introduction

1.1.1 Blaenau Gwent County Borough Council operates a Public Space Closed Circuit Television (CCTV) system (hereafter called the PS CCTV System). The PS CCTV System comprises of a number of cameras installed at strategic locations in the county borough. All the cameras are fixed cameras with no facility to pan, zoom or tilt. The system is currently 'record-only' with no 'live' monitoring taking place. The footage is normally accessed via the CCTV Control Room in the Civic Centre, Ebbw Vale.

1.1.2 For the purposes of this document, the PS CCTV System is owned and managed by Blaenau Gwent County Borough Council. The responsibility for the overall management of the PS CCTV System lies with the Nominated Chief Officer who oversees the effective day-to-day management of the control room and the PS CCTV System.

1.1.3 For the purposes of the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act 2018 the 'data controller' is Blaenau Gwent County Borough Council.

1.1.4 Blaenau Gwent County Borough Council is registered with the Information Commissioner's Office (ICO) under registration reference Z6623658.

1.1.5 Details of the telephone numbers of the owners of the PS CCTV System, together with their respective responsibilities, are shown at Appendix A to this Code.

1.2 Statement in respect of The Human Rights Act 1998

1.2.1 The Council recognises that Public Authorities and those organisations carrying out the functions of a public service are required to observe the obligations imposed by the Human Rights Act 1998. The Council considers that the use of CCTV in Blaenau Gwent is a necessary, proportionate and appropriate measure to help reduce crime, deter anti-social behaviour and to improve public safety.

1.2.2 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. Closed circuit television is also considered a necessary initiative by the Council under their duty to the Crime and Disorder Act 1998.

1.2.3 It is recognised that the operation of the Blaenau Gwent County Borough Council PS CCTV System may infringe on the privacy of individuals. The Council recognises that it is their responsibility to ensure that the PS CCTV

System should always comply with all relevant legislation, to ensure its legality and legitimacy.

1.2.4 The PS CCTV System will only be used as a proportionate response to identified problems and be used only insofar as it is necessary in a democratic society, in the interests of national security, 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.

1.2.5 Observance of this Code and the accompanying PS CCTV Procedure Manual shall ensure that evidence is secured, retained and made available as required with due regard to the rights of the individual.

1.2.6 The Blaenau Gwent County Borough Council PS CCTV System shall be operated with respect for all individuals, recognising the individual right to be free from inhuman or degrading treatment and avoiding any form of discrimination on the basis of age, disability, gender, race, religion or belief, sexual orientation, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.3 Objectives of the System

1.3.1 The objectives of the Blaenau Gwent County Borough Council PS CCTV System, which form the lawful basis for the processing of data, are:

- The preservation of life and limb, to minimise the risk of harm to the vulnerable and public at large.
- The prevention and detection of crime.
- The investigation of crime by identifying offenders, potential victims and witnesses.
- The prosecution of offenders.
- The tendering of video and still images in evidence to the Police, other Law Enforcement Agencies and relevant Local Authority Departments for use in the Criminal Justice System.
- To reduce Anti-Social Behaviour.
- To promote the objectives of Gwent's Police and Crime Commissioner's Police and Crime Plan 2017-2021 and the Blaenau Gwent Community Safety Hub, to make Blaenau Gwent a safer place to live, work and visit.

1.4 Public Space CCTV Procedure Manual

1.4.1 This Code of Practice will be supplemented by a separate Public Space CCTV Procedure Manual, which will provide guidelines on all aspects of the day-to-day operation of the PS CCTV System. To ensure the purpose and principles (see Section 2) of the PS CCTV system are realised, the PS CCTV Procedure Manual is based upon and expands the contents of this Code of Practice. (This will not be a public document.)

Section 2 Statement of Purpose and Principles

2.1 Purpose

2.1.1 The purpose of this document is to state the intention of the PS CCTV System owners and managers, as far as is reasonably practicable to support the objectives of the Blaenau-Gwent County Borough Council PS CCTV System and to outline how it intends to do so.

2.2 The General Principles of Operation

2.2.1 The PS CCTV System will be operated in accordance with the principles and requirements of the Human Rights Act 1998.

2.2.2 The operation of the PS CCTV System will also recognise the need for formal authorisation of any covert 'directed surveillance', as required by the Regulation of Investigatory Powers Act (RIPA) 2000.

2.2.3 The PS CCTV System will be operated with due regard to the relevant definitions, rules and procedures in the Home Office Code of Practice "Covert Surveillance and Property Interference" including updates published from time to time.

2.2.4 Covert surveillance conducted by the Council is outside the scope of this Code and is dealt with by a separate policy statement.

2.2.5 The PS CCTV System will be operated in accordance with General Data Protection Regulation (GDPR) 2016, the Data Protection Act 2018, and the Protection of Freedoms Act 2012.

2.2.6 The PS CCTV System will be operated fairly and within the law. It will only be used for the purposes for which it was established and which are identified within the Code of Practice, or which may be subsequently be agreed in accordance with the Code of Practice.

2.2.7 The PS CCTV System will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and home.

2.2.8 The public interest in the operation of the PS CCTV System will be recognised by ensuring the security and integrity of operational procedures.

2.2.9 Throughout this Code of Practice, it is intended, as far as reasonably possible, to balance the objectives of the PS CCTV System with the need to safeguard the rights of the individual. The owners of the PS CCTV System operate a corporate complaints procedure, and have in place the

appropriate checks and balances with clear lines of accountability for the PS CCTV System.

2.2.10 Involvement with the PS CCTV System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this Code of Practice and to be accountable under the Code of Practice.

2.3 The Surveillance Camera Commissioner's Code of Practice

2.3.1 As per Section 30 (1) (a) of the Protection of Freedoms Act 2012, the PS CCTV System owners and operators must follow a duty to have regard to the Surveillance Camera Commissioner's Code of Practice and the 12 guiding principles contained within:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

2.4 Copyright and Data Controller

2.4.1 Copyright and ownership of all material recorded by virtue of the PS CCTV System will remain with the Data Controller – the Council.

2.4.2 The PS CCTV System owner (the Council) is the data controller for the purposes of the Data Protection Legislation. Once recorded data has been disclosed to another party, such as the Police, they may then become a 'controller in common' for the processing of that data independently of the CCTV System owner. Both parties should exercise all due diligence in ensuring compliance with the Data Protection legislation.

2.5 Cameras and Area Coverage

2.5.1 The areas covered by PS CCTV to which this Code of Practice refers are the public areas within Blaenau Gwent County Borough. The System is currently divided into 7 distinct zones - Ebbw Vale, Tredegar and Cefn Golau, Brynmawr, Abertillery, Blaina, Cwm, and Llanhilleth Railway Station. The System may be expanded to cover any area within the boundaries of Blaenau Gwent County Borough Council.

2.5.2 Deployable or mobile cameras may be temporarily sited within Blaenau Gwent. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the System and is governed by this PS CCTV System Code of Practice and the PS CCTV System Procedure Manual.

2.5.3 All of the PS CCTV System cameras offer a full colour and fixed view capability, using a variety of 'bullet' cameras, 180° Panoramic, Turret and 4G Mobile cameras some of which may automatically switch to monochrome in low light conditions.

2.5.4 None of the cameras forming part of the PS CCTV System will be installed in a covert manner. Some cameras may be enclosed within 'all weather domes', for aesthetic or operational reasons, but appropriate bi-lingual signage will identify the presence of all cameras.

2.5.5 The locations of all cameras within the PS CCTV System are published on the Blaenau Gwent Council website at www.blaenau-gwent.gov.uk

2.6 Monitoring and Recording Facilities

2.6.1 The footage is normally accessed via the Public Space CCTV Control Room which is located in the Civic Centre, Ebbw Vale. It can also be accessed remotely in extenuating circumstances or for technical and maintenance purposes.

2.6.2 The PS CCTV System equipment has the capability of recording all cameras simultaneously throughout every 24-hour period.

2.6.3 PS CCTV System operators are able to record images from selected cameras, produce hard copies and digital copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code of Practice. Only trained and authorised users shall operate viewing, recording equipment and handle any downloaded data.

2.7 Human Resources

2.7.1 A register of all designated PS CCTV System Operators will be maintained by the SIRO.

2.7.2 All Designated PS CCTV System Operators shall receive relevant training and should have requisite knowledge in the requirements of the:

- Human Rights Act 1998,
- General Data Protection Regulation (GDPR) 2016,
- Data Protection Act 2018,
- Regulation of Investigatory Powers Act (RIPA) 2000,
- Surveillance Camera Commissioner's Code of Practice, and this
- Code of Practice and the PS CCTV Procedure Manual.

2.7.3 Further training will be identified and provided as necessary.

2.8 Processing and Handling of Recorded Material

2.8.1 All recorded material will be recorded in digital format and will be processed and handled strictly in accordance with the Code of Practice and the PS CCTV System Procedure Manual.

2.9 CCTV Operators' Instructions

2.9.1 Technical instructions on the use of equipment housed within the PS CCTV Control Room are contained in a separate manual provided by the equipment suppliers.

2.10 Changes to the Code of Practice or the Procedure Manual

2.10.1 Any major changes to this Code of Practice or the PS CCTV System Procedure Manual, i.e. changes that have a significant impact upon the Code of Practice or upon the operation of the PS CCTV System, will be considered and authorised by annual review process.

2.10.2 Minor changes, such as may be required for clarification and which will not have a significant impact, will be included in this Code of Practice and the PS CCTV System Procedures Manual without requiring higher authorisation.

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 Although members of the public have become accustomed to being observed, those who do express concern do so mainly over matters relating to the processing of the information, or data, i.e. what happens to information that is obtained?

Note: 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction or the information or data.

3.1.2 All personal data obtained by virtue of the PS CCTV System shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the PS CCTV System. When processing personal data, the individual right to privacy in their private and family life and home will be respected. Blaenau Gwent County Borough Council's lawful basis for processing data is for the performance of a task carried out in the public interest.

3.1.3 Data will be stored securely in accordance with the requirements of the General Data Protection Regulation (GDPR) 2016 and the Data Protection Act 2018.

3.1.4 Data Protection Impact Assessments will be completed for the respective PS CCTV zones, and will be reviewed annually to ensure that privacy and data protection concerns are appropriately addressed.

3.1.5 Cameras will not be used to look into private residential property. 'Privacy zones' are programmed into the PS CCTV System which prevent the cameras from looking in private residence. In addition, all operators will be specifically trained on issues in relation to privacy.

3.1.6 A member of the public wishing to register a complaint about any aspect of the PS CCTV System may do so by contacting Blaenau Gwent County Borough Council. All complaints shall be dealt with in accordance with the Council's Corporate Complaints Procedure. Any disciplinary issue identified will be considered under the Council's disciplinary procedures.

3.1.7 All contracted or directly employed PS CCTV System staff are contractually bound by regulations governing confidentiality and discipline.

3.2 Data Protection Legislation

3.2.1 For the purposes of the Data Protection Act 2018 the 'Data Controller' is the Blaenau Gwent County Borough Council.

3.2.2 All personal data will be processed in accordance with the six principles of the General Data Protection Regulation (GDPR) 2016, which must be:

1) All personal data will be obtained and processed fairly and lawfully.
2) Personal data will be held only for purposes specified.
3) Personal data held will be adequate, relevant and not excessive in relation to the purpose for which the data is processed.
4) Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
5) Personal data will be held for no longer than is necessary.
6) Personal data will be processed in accordance with the rights of the individual data subject.

3.2.3 In addition – appropriate measures will be taken to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

Personal data will not be transferred to countries outside the European Economic Area unless there is an adequate level of protection for the rights and freedom of data subjects in place in the intended destination.

3.3 Disclosing personal information – exemptions under the Data Protection legislation

3.3.1 Certain exemptions allow for the disclosure of personal data in situations where there would otherwise be a breach of the Data Protection legislation, or allow information to be withheld from Data Protection legislation, or allow information to be withheld from data subjects in circumstances in which it would otherwise need to be disclosed.

3.3.2 The more commonly deployed exemptions are:

1) the disclosure is necessary for the purposes of preventing or detecting crime and the apprehension or prosecution of offenders;
2) the disclosure is necessary for the purposes of maintaining effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control;
3) the disclosure is required by an enactment, rule of law or court/tribunal order;
4) the disclosure is necessary for the purposes of actual of prospective legal proceedings, or obtaining of legal advice or establishing, exercising or defending of legal rights.

3.3.3 Processing personal data is exempt from the subject access provisions to the extent to which the application of those provisions to the data would be likely to prejudice any of the purposes referred to above.

3.4 Disclosure to the Police

3.4.1 The disclosure of recorded data will be on the authority of the Nominated Chief Officer and dealt with in accordance with the PS CCTV Procedure Manual.

3.4.2 Disclosure will be in accordance with the Information Sharing Agreement with Gwent Police (when arranged), including the submission of Gwent Police Form - "Request to external organisation for the disclosure of personal data to the Police", which will cite a specified, explicit and legitimate purpose for the disclosure/sharing of data. This means that the reason(s) for each instance of a disclosure (including viewing)/sharing of data must be set out clearly by the Police, including their reliance on any Data Protection legislation exemptions and justification for reliance on the exemptions.

3.4.3 Once an image or images has been disclosed to a partner agency such as the Police, then they become the Data Controller for the copy of that image(s). It is then the responsibility of that partner to comply with General Data Protection Regulation (GDPR) 2016 and the Data Protection Act 2018 in relation to any further disclosures.

3.5 Criminal Procedures and Investigations Act 1996 (CPIA)

3.5.1 The Criminal Procedures and Investigations Act 1996 introduced a statutory framework for the disclosure to defendants of material that the prosecution would not intend to use in the presentation of its own case. This material is known as 'unused material'. A summary of the provisions of the Act is contained within the PS CCTV Procedure Manual, but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 45 of the Data Protection Act 2018, known as subject access.

3.6 Disclosure to Insurance Companies

3.6.1 The disclosure of recorded data will be on the authority of the PS CCTV Supervisor and dealt with in accordance with the PS CCTV Procedure Manual.

3.6.2 A request can be made by emailing cctv@blaenau-gwent.gov.uk. The relevant form will be forwarded and the request will be dealt with once payment for disbursements (a minimum fee of £50) is received by the PS CCTV System Owner. All information regarding the footage will be logged in the PS CCTV Control Room Data log.

3.7 Disclosure to the Media

3.7.1 The Data Protection legislation exemption (Schedule 2, part 5, para 26(3) of the Data Protection Act 2018) applies to journalism but this should not be construed as an automatic blanket exemption from the Data Protection legislation -the media must still ensure they give consideration to the data protection rights of individuals.

3.7.2 The CCTV System Owner must be satisfied that the disclosure is lawful, sufficiently justified in the public interest and would be fair and meet the 'legitimate interests' condition. If the information in question is sensitive personal data (someone's health, sex life or allegations of criminal activity), there is a specific Data Protection legislation condition to allow a public interest disclosure to journalists if it is related to wrongdoing or incompetence, but otherwise, the CCTV System Owner will need to be satisfied that one of the conditions for processing sensitive data applies. The key is proportionality. It is a balancing act – if there is a serious privacy intrusion or risk of harm, the media will need to demonstrate/establish a significant public interest to justify the disclosure.

3.7.3 The Data Protection legislation does not oblige the CCTV System Owner to disclose information to the media, if it disagrees with the media's view of the public interest, or if the CCTV System Owner has other overriding legal, professional or reputational reasons to refuse to disclose the information.

3.7.4 *Before disclosing information to the media, the CCTV System Owner must ensure that the request cites an appropriate public interest justification.*

3.8 Request for information (Subject Access Requests)

3.8.1 Personal data includes CCTV images of an individual, or images, which gives away information about an individual, such as their car number plate.

3.8.2 An individual is only entitled to their own data, and not to information relating to other people, (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that the PS CCTV System owner establishes whether the information requested falls within the definition of personal data. For further information about the definition of personal data please see the ICO Right of Access Guidance on what is personal data.

3.8.3 The Data Protection legislation does not prevent an individual making a subject access request via a third party such as a solicitor. In these cases, the PS CCTV System owner will need to satisfy itself that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

3.8.4 A child can also request access to information held and shared. Even if a child is too young to understand the implications of subject access rights, it still has the right rather than anyone else such as parent or guardian. So, it is the child who has a right of access to the information held about them, even though in the case of young children, these rights are likely to be exercised by those with parental responsibility for them.

3.8.5 Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual (perhaps a perpetrator). The PS CCTV System owner can refuse to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

a) the other individual has consented to the disclosure, or
b) it is reasonable to comply with the request without that individual's consent.

3.8.6 In determining whether it is reasonable to disclosure the information, the PS CCTV System owner must consider all the relevant circumstances including:

- the type of information that it would disclose;
- any duty of confidentiality owed to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent and
- any express refusal of consent by the other individual.

3.8.7 This means that although the PS CCTV System owner may sometimes be able to disclose information relating to a third party, it needs to decide whether it is appropriate to do so in each case. The decision will involve balancing the data subject's rights of access against the other individual's rights. If the other person consents to the disclosure of information about them, then it would be unreasonable not to do so. However, if there is no such consent, the PS CCTV System owner must decide whether to disclose the information anyway.

3.8.8 Under Data Protection legislation, it is an offence to make any amendment with the intention of preventing its disclosure.

3.8.9 Any personal access request from an individual for the disclosure of their personal data, which they believe is recorded by virtue of the PS CCTV System, will be directed in the first instance to the Nominated Chief Officer and dealt with by an appropriate Designated CCTV Officer, in accordance with the Data Protection legislation.

3.8.10 In supplying the footage, care must be taken not to disclose any personal data of another individual. This may involve 'blurring' or 'pixilating' parts of the footage such as figures or licence plates.

3.8.11 The information will be provided free of charge. However, a reasonable fee based on the administrative cost of providing the information may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. A reasonable fee may also be charged to comply with requests for further copies of the same information.

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

3.8.13 When responding to a subject access request, the Council cannot apply a policy of blanket non-disclosure. There must be a selected and targeted approach to non-disclosure based on the circumstances of the particular case.

3.8.14 The rights of data subjects are qualified rights and are not absolute. The Data Protection legislation recognises that in some circumstances, the Council might have a legitimate reason for not complying with a subject access request, so it provides a number of exemptions & restrictions from the duty to do so.

The most commonly deployed exemptions are:

- where the information is subject to legal or litigation privilege;
- where the information contains the personal data of a third party;
- where the information is of the type, which would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders if disclosed.

3.8.15 Where an exemption or restriction applies to the facts of a particular request, the Council may refuse to provide all or some of the information requested, depending on the circumstances. The application of exemptions/restrictions must be undertaken in consultation with Legal Services.

3.8.16 Requests by third parties for disclosure of personal data third may include, but are not limited to:

- Police (civil police, British Transport Police, Ministry of Defence Police, or Military Police)
- Statutory authorities/bodies with powers to prosecute, (e.g. H.M Customs and Excise, Trading Standards etc.)
- Solicitors
- Insurance agencies.

3.8.17 Requests by third parties are dealt with in accordance with Section 9 and Appendix C of this Code.

3.9 Requests by Council employees and members of the public – alleged incidences on PS CCTV System Owner's premises

3.9.1 Requests may be made by the PS CCTV System Owner's employees and members of the public for CCTV footage of activity in/on the PS CCTV System Owner's premises e.g. car parks where criminal damage to vehicles is being alleged.

3.9.2 The ICO advises that consideration should be given to whether the request is genuine and whether there is any risk to the safety of the other people involved.

3.9.3 The Council is in no position to accurately assess the risk posed to individuals when PS CCTV footage is requested by a private person or group. Routinely the council will only disclose to approved and authorised third parties such as Police and Insurance Companies and will only consider requests by other parties in rare circumstances where it is clear there is no risk to others. This has no effect on the policy in regards to Data Subject Access Requests.

3.9.4 Vehicle crime should be reported by the individual to Gwent Police and/or to their insurance agency.

3.9.5 Any request from an individual for confirmation as to whether or not personal data concerning them is being processed and, where that is the case, access to the personal data will be directed in the first instance to the Data Protection Officer. Each request will be assessed on its own merits.

3.9.6 The principles of Sections 45 of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016 Article 15 (Rights of Data Subjects and others) shall be followed in respect of every request.

3.9.7 Any person making a request must be able to prove his identity and provide sufficient information to enable the data to be located. For further information on Subject Access Requests please see **here**.

Section 4 Accountability and Public Information

4.1 The Public

4.1.1 Public access to the PS CCTV Control Room will be prohibited. However, in the interest of openness and accountability anyone wishing to visit the Control Room may make a request to the Nominated Chief Officer for written authority to do so. Visitors will always be accompanied by one of the Designated CCTV Officers. Although a visit will only take place in the presence of a designated CCTV Operator, he or she will not be expected to take responsibility for such a visit but will record the visit as follows:

- Date, time and duration of visit
- Names and status of visitors
- Purpose and/or justification of visit.

4.1.2 All visitors will be entered into the Log book by the PS CCTV Operator on duty who will inform visitors of the requirement for a Declaration of Confidentiality. No visits will take place or continue whilst a live incident is running.

4.2 Public Space CCTV System Owner

4.2.1 The CCTV System owner is Blaenau Gwent County Borough Council.

4.3 The Senior Information Risk Officer (SIRO)

4.3.1 The Senior Information Risk Officer (SIRO) will perform the role of Senior Responsible Officer (SRO).

4.3.2 The SIRO is responsible for authorising overt surveillance utilising the PS CCTV System and the Deployable mobile cameras. They are also responsible for authorising any changes to the PS CCTV System affecting the views or scope of the PS CCTV System via the submission of a Data Protection Impact Assessment.

4.3.3 The SIRO is responsible for agreeing any significant changes to this Code of Practice and the PS CCTV Procedure Manual.

4.4 Data Controller

4.4.1 The Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

4.4.2 Blaenau Gwent County Borough Council is registered with the Information Commissioner's Office (ICO) as a Data Controller.

4.5 Nominated Chief Officer (CCTV)

4.5.1 The Nominated Chief Officer is the nominated representative on behalf of the Owner whose role will include responsibility to:

- Have unrestricted access to the Control Room and will receive reports at agreed periods from the CCTV System Manager.
- Liaise with the SIRO to consult with regard to changes to any of its aspects of the CCTV System, including this Code of Practice and the PS CCTV Procedure Manual.
- Ensure that statistical and other relevant information, including any complaints made, will be included in the Annual Report of Blaenau Gwent County Borough Council, and will be made available to the public, Elected Members and other relevant stake holders.

4.6 CCTV System Manager

4.6.1 The Nominated Chief Officer will identify a CCTV System Manager. The System Manager will have delegated authority for data control on behalf of the Data Controller, who will:

- Maintain day to day management of the System as a whole.
- Accept overall responsibility for the System and for ensuring that the Code and requirements of the Procedural Manual are complied with.
- Ensure that every complaint is dealt with in line with the Corporate Complaints Policy.

4.7 Designated CCTV Officers

4.7.1 The designated CCTV Officers will have day-to-day access to the PS CCTV System. They will consist of suitably trained staff as identified by the Nominated Chief Officer.

4.8 Public Information

4.8.1 This Code of Practice - A copy shall be published on the Council's website and will be made available to anyone on request.

4.8.2 Annual Report - A copy of the Annual Report shall be published on the Council's website and will be made available to anyone requesting it.

4.8.3 Signs – Bilingual (Welsh and English) signs will be placed in the locality of the cameras and at main entrance points to the relevant areas, e.g. pedestrian precincts. The signs will indicate:

- The presence of CCTV recording;
- The 'owners' of the CCTV System;
- The contact telephone number; and
- The purpose of the CCTV System.

Section 5 Assessment of the Public Space CCTV System and Code of Practice

5.1 Evaluation

5.1.1 The PS CCTV System will be evaluated periodically to establish whether the objectives of the PS CCTV System are being met. The evaluation will normally include, but not be limited to the following:

- An assessment of the impact upon crime and Anti-Social Behaviour;
- An assessment of the incidents recorded by the System, to include where possible an assessment of the value of evidence provided, and the outcomes of investigations;
- An assessment of the impact on town centre businesses;
- An assessment of neighbouring areas without PS CCTV;
- A review of the Code of Practice and PS CCTV Procedure Manual;
- A review of the continuing relevancy of the objectives of the PS CCTV System; and
- Any other factors - such as PS CCTV System security checks.

5.1.2 The results of any evaluation will be published as part of the Annual Report and will be used to review, develop and make any alterations to the specified purposes and objectives of the scheme as well as the functioning, management and operation of the System.

5.2 Monitoring

5.2.1 The Nominated Chief Officer will be responsible for the operation and evaluation of the PS CCTV System, and the implementation of this Code of Practice.

5.2.2 The Designated Officers shall be responsible for maintaining full management information of incidents dealt with by the PS CCTV Control Room, for use in managing the PS CCTV System and in future evaluations. These and any other issues with the PS CCTV System will be logged and reported to the Senior Information Risk Owner (SIRO).

5.3 Audit

5.3.1 Blaenau Gwent Council's Audit Managers, or nominated deputies, who are not Designated Officers, will be given full access to the System when requested.

5.4 Lay Visitors

5.4.1 An independent panel of community volunteers, may be appointed to carry out periodic visits to the PS CCTV Control Room. Accredited lay visitors will be allowed access to the Control Room at all times unless operational conditions prohibit this.

5.4.2 The purpose of such lay visits is to ensure that, within the constraints of the Data Protection legislation and other relevant legislation, the PS CCTV System and its management and operation remain as open as possible to public scrutiny.

5.4.3 Lay visitors will be required to be conversant with this Code of Practice and the PS CCTV Procedure Manual.

5.4.4 Accredited lay visitors will be asked to monitor PS CCTV Operators' and managers' adherence to this Code of Practice and the PS CCTV Procedure Manual and to report any contravention to the Designated Officers.

5.4.5 Lay visitors will be required to sign a Declaration of Confidentiality and to abide by this Code of Practice at all times. (See Appendix D)

5.4.6 Normally, no more than two lay visitors will visit the PS CCTV Control Room at any one time. They will be required to have their personal details entered into the PS CCTV Control Room Log book and will, as far as practicable, be accompanied by a Designated CCTV Officer.

Section 6 Human Resources

6.1 The Public Space CCTV Control Room and those responsible for the operation of the System

6.1.1 Only authorised personnel who have been trained to use the PS CCTV System's equipment and in the PS CCTV Control Room procedures will operate the PS CCTV System.

6.1.2 Every person involved in the management and operation of the PS CCTV System will be personally issued with a copy of both the Code of Practice and the PS CCTV Procedure Manual. They will be required to sign to confirm understanding of and adherence to the obligations that these documents place upon them and that any breach will be considered a disciplinary offence contrary to the Code of Conduct. He or she will be fully conversant with the contents of both documents, which may be updated from time to time. They will comply with both documents as far as is reasonably practicable.

6.1.3 All persons involved with the PS CCTV System shall receive training in respect of the PS CCTV Code of Practice, the PS CCTV Procedure Manual and legislation relevant to their role. Such training will be updated as and when necessary.

6.2 Discipline

6.2.1 Each individual having responsibility under the terms of the Code of Practice, who has any involvement with the PS CCTV System to which it refers, will be subject to the Authority's Disciplinary Code. Any breach of the Code of Practice, or of any aspect of confidentiality, will be dealt with in accordance with that Authority's Disciplinary Code.

6.2.2 The Designated Officers will have primary responsibility for ensuring that there is no breach of security and that the Code of Practice is complied with. The Designated Officers will have day-to-day responsibility for the PS CCTV Control Room and for adhering to the Code of Practice. Non- compliance with the Code of Practice by any person will be considered a breach of conduct and will be dealt with accordingly, including, if appropriate, by criminal proceedings.

6.3 Declaration of Confidentiality

6.3.1 Every individual with responsibility under the terms of this Code of Practice, who has any involvement with the PS CCTV System to which it refers, will be required to sign a separate declaration of confidentiality. See Appendix B.

6.3.2 Police Officers visiting the PS CCTV Control Room for operational purposes must agree to the declaration of confidentiality by completing and signing the Visitor Log Book.

Section 7 Control and Operation of Public Space CCTV System

7.1 Guiding Principles

7.1.1 All persons operating the PS CCTV System must act with the utmost probity and integrity at all times.

7.1.2 Only persons, who have been trained in their use and the legislative implications of such use, will operate the cameras and the recording and reviewing equipment.

7.1.3 Every use of the cameras will accord with the purposes and key objectives of the PS CCTV System and shall be in compliance with this Code of Practice.

7.1.4 Cameras will not be used to look into private residential properties. 'Privacy zones' have been programmed into the PS CCTV System, whenever practically possible, in order to ensure that any interior of any private residential property is not surveyed by the cameras.

7.1.5 The PS CCTV System has been set up on a 'record only' basis with no 'live-monitoring' taking place, however the PS CCTV System has the facility to 'live-monitor' all cameras but this will only be used in the event of exceptional and emergency circumstances.

7.1.6 Temporary 'Live- monitoring' may take place and be unavoidable when conducting essential maintenance or testing of the PS CCTV System.

7.1.7 In the event of any 'live-monitoring' having to taking place camera operators will have no ability to pan, zoom or tilt any cameras on the System. All cameras have a fixed view which cannot be moved by the operator.

7.1.8 Camera operators must always be mindful of exercising prejudices, which may lead to complaints of the PS 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 or group of individuals or property.

7.2 Public Space CCTV Control Room

7.2.1 Only staff that are trained and authorised to use the CCTV equipment will have access to the PS CCTV System.

7.3 Operation of the Public Space CCTV System by the Police

7.3.1 Under some circumstances the Police may make a request to assume direction of the PS CCTV System to which this Code of Practice applies. Any requests must be made in writing by a police officer not below the rank of Superintendent. Any such request will only be allowed on the written authority of the Managing Director, or the Senior Information Risk Owner (SIRO).

7.3.2 In the event of such a request being allowed, the PS CCTV Control Room will be operated by those personnel who are authorised to do so and who fall within the terms of Sections 6 and 7 of this Code of Practice. They will then operate under the direction of the Police Officer designated in the written authority.

7.3.3 In extreme circumstances a request may be made by the Police to take total control of the PS CCTV System, including the staffing of the PS CCTV Control Room and control of all associated equipment, to the exclusion of all representatives of the PS CCTV System owners. Any such request must be made to the Designated Officers in the first instance, who will consult personally with the Nominated Chief Officer and SIRO. A request for total exclusive control must be made in writing by a Police Officer not below the rank of Superintendent or person of equal standing. A member of the PS CCTV team will be present at all time during the takeover of the facility.

7.4 Maintenance of the PS CCTV System

7.4.1 To ensure compliance with the Surveillance Camera Commissioner's Code of Practice and to ensure that images recorded continue to be of an appropriate evidential quality, the PS CCTV System shall be maintained in accordance with the requirements of the PS CCTV Procedural Manual under a maintenance Service Level Agreement.

7.4.2 The maintenance Service Level Agreement will make provision for regular or periodic service checks on the equipment. This 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.

7.4.3 The maintenance Service Level Agreement will also include provision for regular periodic review and overhaul of all the equipment and replacement of equipment, which is reaching the end of its serviceable life.

7.4.4 The maintenance Service Level Agreement will also provide for ‘emergency’ attendance on site by a specialist CCTV engineer to rectify any loss or severe degradation of image or camera control.

7.4.5 The maintenance Service Level Agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem, depending upon the severity of the event, and the operational requirements of that element of the PS CCTV System.

7.4.6 It is the responsibility of the Nominated Chief Officer to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the contracted maintenance organisation.

Section 8 Access to, and Security of the CCTV Control Room and Associated Equipment

8.1 Authorised Access

8.1.1 Only trained and authorised personnel will operate the equipment located within the PS CCTV Control Room or equipment associated with the 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 Managing Director or Senior Information Risk Owner (SIRO). Any such visits will be conducted and recorded in accordance with the PS CCTV Procedure Manual.

8.3 Authorised Visits

8.3.1 Visits by lay visitors or inspectors or auditors do not fall within the scope of the above paragraph and may take place at any time, without prior warning. No more than two inspectors or auditors may visit at any one time. Inspectors or auditors will not influence the operation of any part of the PS CCTV 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 PS CCTV Control Room, including inspectors and auditors, will be required to have their personal details entered into the Visitor's Book and read and sign a declaration of confidentiality.

8.5 Security

8.5.1 In the event of the PS CCTV Control Room having to be evacuated for safety or security reasons, the provisions of the Procedure Manual will be complied with. The PS CCTV Control Room will be secure at all times by 'Magnetic-Locks' and access will only be gained via a Designated Officer's unique electronic identification card and its authorised permission.

8.6 Airwaves Radio

8.6.1 Due to the PS CCTV System being a 'record-only' system with no 'live-monitoring' (except in exceptional circumstances) Designated Officers are not currently issued with Airwaves Radio to communicate directly with the Police. No Airwaves Radios will be stored at the PS CCTV Control Room. The Code of Practice and PS CCTV Procedure Manual can be adapted should this change in the future.

Section 9 Management of Recorded Material

9.1 Guiding Principles

9.1.1 For the purposes of this Code of Practice 'recorded material' means any material recorded by, or as the result of, technical equipment, which forms part of the PS CCTV System. This specifically includes images recorded digitally or by way of data copying, including still prints.

9.1.2 Every video or digital recording obtained using the PS CCTV System has the potential of containing material that can be admitted in evidence in proceedings in the Criminal Justice System.

9.1.3 Members of the community must have complete confidence that information about their ordinary, everyday activities recorded on the PS 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 of the utmost importance that, irrespective of the means or format of the images obtained from the PS CCTV System, e.g. Paper Copy, Hard Copy Disc Drive, DVD, CD or any form of electronic processing and storage is treated strictly in accordance with the PS CCTV Code of Practice and the PS CCTV Procedure Manual. This applies from the moment they are recorded until their final destruction. Every movement and usage will be recorded.

9.1.5 Recorded material will not be copied, sold, otherwise released or used for commercial purposes of any kind other than for legitimate third party/insurance requests.

9.2 Disclosure of Data to a Third Party

9.2.1 Every request for the release of personal data generated by the PS CCTV System will be channelled through the CCTV System Manager, who will ensure that the principles contained within Appendix C to this PS CCTV Code of Practice are followed at all times.

The disclosure of personal data for commercial or entertainment purposes is specifically prohibited.

9.2.2 In complying with the National Standard for the Release of Data to Third Parties, it is intended, as far as is reasonably practicable, to safeguard the rights of the individual to privacy and to give effect to the following principles:

- recorded material shall be processed lawfully and fairly, and be used only for the purposes defined in this Code of Practice;
- access to recorded material will only take place in accordance with the standards outlined in Appendix C and this Code of Practice; and
- The release or disclosure of Personal Data for commercial or entertainment purposes is specifically prohibited.

9.2.3 Members of the Police Service or other Law Enforcement Agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix C, release details of recorded information to the media in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded in accordance with the PS CCTV Procedure Manual.

Note: The Police and Criminal Evidence Act (PACE) 1984, covers release to the media of recorded information, in any format, which may be part of a current investigation. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial. Full details of any media coverage must be recorded and brought to the attention of both the prosecutor and the defence.

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

9.3 Digital System- Provision & Quality

9.3.1 To ensure the quality of footage, and that recorded information meets the criteria outlined by current Home Office guidelines, only media of good quality are used on the PS CCTV System.

9.4 Information – Retention

9.4.1 Recorded media which has been preserved after a lawful request will be retained for a maximum period of 6 months for collection, or to establish if "non-evidential" or similar. Deletion or destruction will take place in accordance with the manufacturer's requirements and full details of all material deleted or destroyed will be logged.

9.5 Recording Policy

9.5.1 Subject to the equipment functioning correctly, images from most cameras will be recorded throughout every 24-hour period for a period of 31 days after which the data is automatically overwritten unless requested and preserved for a lawful purpose.

9.5.2 Subject to the equipment functioning correctly, images from a few cameras on the PS CCTV System will be recorded for a period of no longer than 7 days after which the data is automatically overwritten. The locations of these cameras presents technical difficulties preventing the data being retained for longer periods without it being downloaded and preserved.

9.6 Evidence Provision

9.6.1 In the event of images being required for evidential purposes the procedures outlined in the PS CCTV Procedure Manual will be strictly complied with.

Section 10 Digital Still Photographs

10.1 Guiding Principles

10.1.1 A digital still photograph is a copy of an image or images which already exist on a computer disc. Such still images are within the definitions of ‘data’ and ‘recorded material’.

10.1.2 Digital still photographs will not be taken as a matter of routine. When a still image is recorded, it must be capable of justification by the originator, who will be responsible for recording the full circumstances under which the still is taken, in accordance with the PS CCTV Procedure Manual and including them being individually numbered.

10.1.3 Digital still photographs contain personal data and will therefore only be disclosed under the terms of Appendix C of this Code of Practice- ‘Disclosure of data to third parties’. If stills are released to the media, in compliance with Appendix C, in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the PS CCTV Procedure Manual.

10.1.4 A record will be maintained of all digital still photograph productions, in accordance with the PS CCTV Procedures Manual. The recorded details will include a sequential number, the date, time and location of the incident, the date and time of the production of the print, the identity of the person requesting the print, (if relevant) and the purpose for which the print was taken.

10.1.5 The records of the digital still photographs taken will be subject to audit in common with all other records in the PS CCTV System.

Section 11 Regulation of Investigatory Powers Act 2000 (RIPA)

11.1 Guiding Principles

11.1.1 The Public Space CCTV System Owner has adopted a Policy Statement in relation to the Regulation of Investigatory Powers Act 2000. This Policy Statement complies with the Home Office Covert Surveillance Codes of Practice and is periodically audited by the IPCO (Investigatory Powers Commissioner). An annual report on the use of RIPA is submitted by the Council to the IPCO.

11.1.2 The PS CCTV System Owner does not currently have a joint working protocol in place with Gwent Police with regard to the use of the Public Space CCTV Systems for surveillance authorised by the Regulation of Investigatory Powers Act 2000 (RIPA).

11.1.3 Advice and guidance for Designated CCTV Officers and Police Officers in respect of Public Space CCTV Systems and the Regulation of Investigatory Powers Act of 2000 (RIPA) is reproduced in Appendix E.

Appendix A

Key Personnel and Responsibilities

1. **System Owner**

Blaenau Gwent County Borough Council is the 'System Owner' of the Public Space CCTV system.

Blaenau Gwent County Borough Council,
Municipal Offices, Civic Centre,
Ebbw Vale, NP23 6XB
Tel: 01495 311556

2. Nominated Chief Officer

The Nominated Chief Officer is the nominated representative on behalf of the 'System Owner'; this role is performed by the Head of Governance and Partnerships.

Blaenau Gwent County Borough Council,
Municipal Offices, Civic Centre,
Ebbw Vale, NP23 6XB
Tel: 01495 311556

The Nominated Chief Officer role will include responsibility to:

a) Ensure the provision and maintenance of all equipment forming part of the PS CCTV System in accordance with contractual arrangements, which the owners may from time to time, enter into.
b) Maintain close liaison with the CCTV System Manager.
c) Ensure the interests of the 'System Owners' and other organisations are upheld in accordance with the terms of this Code of Practice.
d) Agree to any proposed alterations and additions to the system, this Code of Practice and/or the Public Space CCTV Procedural Manual.

3. Senior Responsible Officer (SRO) - Senior Information Risk Officer (SIRO)

The role of (SIRO) is performed by the Chief Officer Resources.

Blaenau Gwent County Borough Council,
Municipal Offices, Civic Centre,
Ebbw Vale, NP23 6XB
Tel: 01495 311556

The Senior Information Risk Officer (SIRO) will perform the role of Senior Responsible Officer (SRO), and will be responsible to:

a) complete the Surveillance Camera Commissioner's Self-Assessment Toolkit. Through the questionnaire they should identify any changes to the system, whether the system remains fit for purpose and whether a maintenance contract is still in place for the system.
b) Authorise overt surveillance utilising the PS CCTV System and the Deployable mobile cameras.
c) Authorise any changes to the PS CCTV System.
d) Agree any significant changes to this Code of Practice and the PS CCTV Procedure Manual.

4. CCTV System Manager

The CCTV System Manager is the 'manager' of the Blaenau Gwent County Borough Council PS CCTV System. They have delegated authority for data control on behalf of the 'data controller'.

Blaenau Gwent County Borough Council,
Municipal Offices,
Civic Centre,
Ebbw Vale,
NP23 6XB
Tel: 01495 311556

The CCTV System Manager is responsible for the integrity, security, procedural efficiency and methods of operation of the System, including the gathering, retention and release of CCTV data.

Their role also includes responsibility to

a) accept overall responsibility for the system and for ensuring that this Code of Practice and the Procedure Manual is complied with;
b) provide supervision and training of all Designated CCTV Operators authorised to assist in the operation of the System; and
c) to maintain direct liaison with partners.

5. Designated CCTV Operators

The Nominated Chief Officer and SIRO will identify Designated CCTV Operators to support the CCTV System Manager. The Designated CCTV Operators will be appropriately trained and will be responsible for the integrity, security, procedural efficiency and methods of operation of the System.

Appendix B

Public Space CCTV Control Room System - Declaration of Confidentiality/ Non-Disclosure Agreement

This confidentiality agreement acknowledges that my duties allow me access to the Public Space CCTV Control Room or data processed by the Public Space CCTV System.

I agree that I have read the Code of Practice in respect of the operation and management of the Public Space CCTV System, and hereby declare that I have familiarised myself with the content of that Code of Practice and understand that all duties, which I undertake in connection with the Blaenau-Gwent County Borough Council Public Space CCTV System, must not contravene any part of the current Code of Practice, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the PS CCTV System or the content of the Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that my part in fulfilling the duties of my role means that I may have access to sensitive and personal information and that such access shall include:

- reading or viewing of information held on computer or displayed by some other electronic means,
- reading or viewing manually held information in written, printed or photographic form, or
- overhearing any telephone or verbal communication.

I undertake that:

- I shall not communicate to nor discuss with any other person the contents of the information except to those persons authorised by the Data Controller as is necessary.
- I shall not retain, extract, copy or in any way use any information to which I have been afforded access during the course of my duties for any other purpose.
- I will only operate computer applications or manual systems that I have been instructed to use or given access permissions to access in compliance with the Data Protection Act 2018 which prescribes the way in which personal data may be obtained, stored and processed.
- I will act only under instruction from Senior Management or other relevant officials in the processing of any Data.
- I will comply with the appropriate physical and system security procedures made known to me by the Data Controller.

I understand that any Information is subject to the provisions of the General Data Protection Regulation 2016 and that by knowingly or recklessly acting outside the scope of this Agreement I may incur criminal and/or civil liabilities and subject to the internal disciplinary procedures.

I undertake to seek advice and guidance from Senior Management or other relevant official of the Data Controller in the event that I have any doubts or concerns about my responsibilities or the authorised use of the Data defined in the Agreement.

I have read, understood and accept the above.

In appending my signature to this declaration, I agree to abide by the Code of Practice at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format - now or at any in the future (including such time that I have ceased to be employed by Blaenau-Gwent County Borough Council).

Name:……..

Signature: ……

Witness: ……..

Position: ……..

Date: …….

Appendix C

National Standard for the Release of Data to Third Parties

1. Introduction

1.1 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, CCTV systems must be used with the utmost probity at all times and in a manner, which stands up to scrutiny by the people they are aiming to protect.

1.2 Blaenau Gwent County Borough Council believes that everyone has the right to respect for their private and family life and home. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (data) which the CCTV System gathers. The PS CCTV System Owners are aware of the nationally recommended standard of The CCTV User Group. https://www.cctvusergroup.com/

2. General Policy on disclosure/sharing

2.2 All requests for the release of data shall be processed in accordance with the PS CCTV Procedure Manual. All such requests shall be channelled through the data controller.

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 (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
- 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); and
- v) Identification of witnesses.

b) Third parties, who are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

- i) Police (Note 1 below);
- ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise, Trading Standards, etc.);
- iii) Solicitors (Note 2 below);
- iv) Plaintiffs and defendants in civil proceedings (Note 3 below);

v) Accused persons or defendants in criminal proceedings (Note 3 below); and
vi) Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status. (Note 4 below)

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; and
ii) Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.

d) In circumstances outlined at note 3 below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative, shall:
i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation; and
ii) Treat all such enquiries with strict confidentiality.

Notes:

(**1**) The release of data to the police is not to be restricted to the civil police but could include, for example, British Transport Police, Ministry of Defence Police, or Military Police. (It may be appropriate to put in place special arrangements in response to local requirements).

(**2**) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.

(**3**) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor, falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

(**4**) The data controller shall decide which (if any) ‘other agencies’ might be permitted access to data. Having identified those ‘other agencies’, such access to data will only be permitted in compliance with this Standard.

(**5**) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should be reasonably specific, for example, specified to the nearest half-hour.

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. GDPR and The 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 GDPR and The 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' (Note 1 below)

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 this Code (Note 2 below); and

ii) if the material is to be released under the heading of 'public wellbeing, 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 this Code.

c) Recorded material may be used for bona fide training purposes such as for police or staff training. Under no circumstances will recorded material be released for commercial sale 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 interest to the public well-being;

ii) Identifies a public health or safety issue; and

iii) Assists in 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).

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) No fees will be charged for subject access requests.
iii) The data controller is supplied with sufficient information to satisfy him as to the identity of the person making the request;
iv) Sufficient and accurate information is provided about the time, date and place to enable the data controller to locate the information that the person seeks. It is recognised that a person making a request is unlikely to know the precise time. In such circumstances it is suggested that accuracy to within one hour would be a reasonable requirement; and

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 considered on its own merits.

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, so far as can be reasonably ascertained, not likely to become part of a 'live' criminal investigation;
ii) Not currently and, so 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; and
vi) For individual disclosure only (i.e. to be disclosed to a named subject).

6. Process of Disclosure

a) Verify the accuracy of the request.
b) Replay the data to the requester 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, the material shall be sent to an editing house for processing prior to being sent to the requester.

7. Media disclosure

7.1.1 Set procedures for release of data to a third party must be followed. If the means of editing out other personal data does not exist on-site, measures should include the following:

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;
ii) The release document shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities or data that must not be revealed;
iii) The release document shall require that following editing and prior to its use by the media, the data must be passed back to the data controller, either for final approval or consent to its use. This protects the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System's Code; and
iv) The release document shall be considered a contract and signed by both parties as such. The signatories must have the requisite standing to sign in that capacity on behalf of their respective organisations.

8. Principles

8.1.1 In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code for the CCTV scheme;
b) Access to recorded material shall only take place in accordance with this Standard and the Code; and
c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Appendix D

Confidentiality Agreement Lay Visitors

I am a Lay Visitor of the Blaenau Gwent County Borough Council's Public Space CCTV System with a responsibility to monitor the operation of the System and adherence to the Code of Practice. I have received a copy of the Code in respect of the operation and management of that CCTV System.

I confirm that I am fully conversant with my voluntary duties and the content of the Code of Practice. I undertake to inform the Designated CCTV Officers of any apparent contravention of the Code of Practice that I may note during the course of my visits to the Public Space CCTV Control Room.

If now, or in the future I am, or I become unclear of any aspect of the operation of the CCTV System or the content of the Code of Practice, I undertake to seek clarification of such uncertainties.

I understand that it is a condition of my duties that I do not disclose or divulge any information which I have acquired in the course of, or in connection with, my position as a Lay Visitor to any company, authority, agency, other organisation or any individual. This includes information obtained verbally, in writing or by any other media, now or in the future. I understand that this prohibition remains binding after I have ceased to perform duties as a Lay Visitor.

In signing this declaration, I agree to abide by, and be bound by, the Code of Practice. I understand and agree to maintain confidentiality in respect of all information gained during the course of my voluntary duties, now, or in the future.

Signed:……

Print Name: ……

Witness: …….

Position: …….

Dated the ……. (day) of ……(month) 20…..

Appendix E

Regulation of Investigatory Powers Act (RIPA) Guiding Principles

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

The Regulation of Investigatory Powers Act 2000 (RIPA) relates to surveillance by the Police and other agencies with investigatory powers, and deals in part with the use of directed covert surveillance. Section 26 of this 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 Public Space CCTV Control Room is that there might be cause to monitor for some time a person or premises using the cameras. In most cases, this will fall into sub section (c) above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The Code says some hours rather than minutes.

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

Slow time requests are authorised by a Police Superintendent or above.

If an authorisation is required immediately, a Police Inspector may do so. The forms in both cases must indicate the reason and should fall within one of the following categories:

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 paragraph (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, followed by written confirmation using the forms. Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising.

Forms should be available at the CCTV Control Room and are included in the PS CCTV Procedure Manual and available from the CCTV User Group Website.

Examples:

Inspector's Authorisation

An example of a request requiring an Inspector's authorisation might be where a car is found in a car park late at night and is known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time to note who goes to and from the vehicle.

Superintendent's Authorisation

An example here might be where it is suspected that shop premises are being utilised for dealing stolen goods and officers wish to use the Public Space CCTV to monitor the premises from outside for a period of days.

No Authorisation Required

An example might be where Police Officers chance upon local drug dealers sitting in the town centre and, in order not to divulge that they are being observed they ask CCTV operators to monitor them.