CCTV Code of Practice Policy

1. INTRODUCTION AND OBJECTIVES

1.1 This code of practice has been written in accordance with the Information Commissioner's CCTV Code of Practice and the National Surveillance Commissioner's CCTV Code of Practice.

1.2 This Code of Practice applies to all CCTV cameras operated and managed by Penyffordd Community Council at the Millstone Play Area, Penyffordd and Hawarden Road, Penyffordd.

1.3 The system owner and Data Controller is Penyffordd Community Council. It is responsible for the ownership of the system with overall responsibility for ensuring this Code of Practice is adhered to and the system is properly maintained. The Council are responsible for the day to day management of the system and the management of the code of practice, North Wales Police (Mold Police Station) are the Data Processor responsible for the including data processing and management of the code of practice.

2. STATEMENT IN RESPECT OF HUMAN RIGHTS ACT 1998

2.1 The system owners have considered the obligations imposed by the above legalisation and consider that the use of cameras in the locations mentioned above is necessary proportionate and a suitable tool to help prevent and detect crime and disorder.

2.2 The system will be operated with respect to all individuals, without any discrimination on the grounds of gender, race, colour, language, religion, political opinion, national or social origin or sexual orientation.

3. OBJECTIVES OF THE SYSTEM

3.1 The primary objective of the CCTV system is to protect Community Council owned property and increase the safety of the users of our facilities. To achieve this objective the system will be used and data processed for the following purposes only:

- To prevent and detect crime, providing evidential material for criminal proceedings;
- To deter and detect incidents of anti-social behaviour, providing evidential material for criminal proceedings;
- To assist with other civil proceedings such as insurance claims.

3.2 The need to assist with personal safety will override any other requirements.

4. SYSTEM REVIEW

4.1 The system will be reviewed annually to ensure it remains necessary, proportionate and effective.

5. STATEMENT OF PURPOSE AND PRINCIPLE

5.1 Purpose – The purpose of this document is to state how the Owners and System Manager intend to use the system to meet the objectives and principles outlined in Sections 1 to 4 above.

5.2 General Principles of Operation – The system will be operated in accordance with this Code of Practice and the Data Protection Act 2018 at all times. The system will be operated in due deference to the general right to respect for an individual and regard for their private and family life.

5.3 The public interest in the operation of this system will be safeguarded by ensuring the security and integrity of operational procedures.

5.4 Copyright – Copyright and ownership of all material recorded on the system, will remain with the Data Controller.

5.5 Monitoring and Recording Facilities – The images from the cameras located at the Millstone Play Area and Hawarden Road Penyffordd are stored on the CCTV hard drives and or/on a PC located at Mold Police Station

5.6 The images from the cameras located at the Millstone Play Area and Hawarden Road Penyffordd are stored securely within an encrypted hard drive which can only be accessed by the Data Processor (North Wales Police).

5.7 Processing and Handling of Recorded Material – No record material, whether digital, analogue, hard copy or otherwise will be released by the Data Processor unless it is in accordance with this Code of Practice.

5.8 Changes of this Code of Practice – All changes to this Code will be agreed by the Owners of the system.

6. PRIVACY AND DATA PROTECTION

6.1 Data Protection Legalisation – The operator of the system has been notified to the Office of the Information Commissioners in accordance with the current Data Protection Legalisation. Data will be processed in accordance with the Data Protection Act 2018, summarised as:

- Processed fairly, lawfully and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with the original purpose
- Adequate, relevant and limited to what is necessary in relation to the purposes
- Accurate and kept up to date
- Kept in a form that permits identification no longer than is necessary
- Processed in a way that ensures appropriate security of the personal data

6.2 Subject Access Request – Any request from an individual for disclosure of personal data which they believe is recorded by virtue of the system will be directed in the first instance to the Data Processor and should be treated as a Subject Access Request.

6.3 Any personal making such a request should use the form included as Appendix 2 and must be able to provide sufficient information to prove their identify and enable the data to be located.

6.4 If the relevant footage shows third parties and the provision of such could involve an unfair intrusion into their privacy of the third party, the footage will not be disclosed unless all third parties have provided written agreement of the relevant footage can be obscured.

6.5 In accordance with the Data Protection Act 2018, personal data processed for the prevention of crime and/or the apprehension or prosecution of offenders is exempt from the subject access

provisions, to the extent to which the application of the provisions to the data would be likely to prejudice these matters.

6.6 A request from an individual for footage for themselves is exempt from the provisions of the Freedom of Information Act. Instead this request should be treated as a data protection subject access request as explained above.

7. ACCOUNTABILITY AND PUBLIC INFORMATION

7.1 This Code will be made available on the Council's website and upon request to the Data Controller.

8. ASSESSMENT OF THE SYSTEM

8.1 The operation of the system will be audited on an annual basis to check for compliance with this Code of Practice and to ensure the system meets the objectives specified in section 3.

9. MANAGEMENT OF RECORDED MATERIAL

9.1 Guiding Principles – For the purposes of this Code, 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of this system; this specifically includes images recorded digitally or on other media including still prints.

9.2 Every recording made by the use of the system has the potential for containing material that may need to be admitted in evidence at some point during the period of its retention.

9.3 Members of the public must have total confidence that information recorded will be treated with due respect for private and family life. It is therefore imperative that all recorded is treated strictly in accordance with this Code of Practice until the final destruction of the material.

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

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

10. NATIONAL STANDARD FOR RELEASE OF DATA TO A THIRD PARTY

10.1 Requests from the Police for footage for the prevention and/or detection of crime and disorder will be submitted to the Data Processor.

10.2 In complying with the National Standard it is anticipated, as far as is reasonably practicable, to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in the Code.
- Access to recorded material will only take place in accordance with the National Standard and this Code.

10.3 Subject to compliance with this Code, the Police and other agencies with a Statutory Authority to investigate and/or prosecute offences, may release details of recorded information to the media only in an effort to identify offenders or potential witnesses. In all cases this will need the permission of the Data Controller.

11. RETENTION OF FOOTAGE AND RECORDED MATERIAL

11.1 Images are recorded by cameras are retained on the system for 28 days. After this time, the footage is erased.

11.2 When footage is released as recorded material a master copy is made and retained securely. This is retained for 6 years plus the financial year it is recorded in, after which it is securely destroyed.

12. REGISTER AND RELEASE OF RECORDED MATERIAL

12.1 Every item of recorded material that is produced is managed using specific software which provides a clear audit trail.

12.2 Prints of Recorded Material – Prints will be treated in the same manner as other recorded material and in accordance with this Code of Practice and the National Standard.

This Code of Practice was reviewed and approved at the Annual Meeting held on 10th May 2023

APPENDIX 1 - NATIONAL STANDARD FOR THE RELEASE OF DATA TO THIRD PARTIES

All requests for the release of data shall be processed in accordance with this standard and the Code of Practice. All Police requests for footage needed for the prevention and/or detection of crime and disorder shall be dealt with by the Data Processor. Data to day responsibility for the operation of the CCTV system lies with the Data Processor.

1. 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, Crime Procedures and 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).
   v. The identification of witnesses

(b) Third parties, which are requested to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
   i. Police (see note 1)
   ii. Statutory (enforcing) authorities with powers to prosecute (e.g. Custom & Excise, Trading Standards etc).
   iii. Solicitors (see note 2)
   iv. Plaintiffs in civil proceedings (see note 3)
   v. Accused persons or defendants in criminal proceedings (see note 3)
   vi. Other agencies, according to purpose and legal status (see note 4)

(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 the 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 in 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.
   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, British Military Police, Ministry of Defence Police etc. Special arrangements may be put in place 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 circumstance, 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 legalisation. 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 sufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest half hour).

2. 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 Processor shall ensure that:

i. The request does not contravene and that compliance with the request would not breach current legislation (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Just and Public Order Act 1994 etc.)
ii. Any legislative requirements have been complied with (e.g. the requirements of the Data Protection Act 1998).
iii. Due regard has been taken of any known case law (current or past) which may be relevant
iv. The request would pass a disclosure of 'public interest' (see note 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 releasing 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 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 or for entertainment purposes.

Note

(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.
iii. Leads to the prevention of crime.
iv. 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 3 above)

3. Individual Subject Access under Data Protection Legislation

(a) Under the terms of the Data Protection legalisation, 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 search
iii. The Data Controller is provided with sufficient information to suffice him/herself as to the identity of the person making the request

iv. 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 may not know the precise time. Under these circumstances, it is suggested that within one hour of accuracy would be a reasonable requirement).
v. The personal making the request is only shown information relevant to that particular search and which contains personal data of him/herself 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).

(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 merits.

(d) In addition to the principles 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 or 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 an 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)

4. Process of Disclosure

(a) Verify the accuracy of the request
(b) Replay the data to the requestee only (or a responsible person acting on their behalf.
(c) Only data relating to the request will be shown.
(d) It must not be possible to identify any other individual from the information being shown
(e) If a copy of the material is requested and there is no one site means of editing out other personal data, then the material should be sent to an editing house for processing prior to being send to the requestee.

Note: The Information Commissioner's Code of Practice for CCTV makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.

5. 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 for its use.
ii. The release form shall state that the receiver must process data in a manner prescribed by the data controller e.g. specific identifies/data that must not be revealed.
iii. 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 legalisation and the System Code of Practice).

iv. The release form shall be considered a contract and signed by both parties (see note 1)

Note: In the well case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck (QBD, November 1997), the judge concluded that by releasing the video footage the Council had not acted lawfully. A verbal reassurance that the broadcasters would mast the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be considered to avoid future accidental broadcasts. Attention is drawn in this respect, detailed in her Code of Practice summarised above.

6. Principles

6.1 In adopting a 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 of Practice for the system.

(b) Access to recorded material shall only take place in accordance with this standard and Code of Practice.

(c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

APPENDIX 2 - SUBJECT ACCESS REQUEST FORM

SUBJECT ACCESS REQUEST FORM

Under the Data Protection Act you have a statutory right to request confirmation that the council is processing your data and to request to see information held on you by that organisation.

You also have the right to be told:

- the purposes of and legal basis for the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been disclosed;
- the period for which the personal data is to be held;
- that you have rights to rectification and erasure of personal data where, for example, factual information has been recorded incorrectly;
- that you have the right to lodge a complaint with the Information Commissioner's Office and the contact details of the Commissioner;
- any information about the origin of the personal data concerned.

This information is likely to be available in general terms within our privacy notices, however you can request it in addition to any request to see your records.

To request to see your records, please complete this form, read and sign the declaration and then send the completed form to Penyffordd Community Council, 3 Old Chester Road, Ewloe , Deeside, Flintshire, CH5 3RU

To ensure proper security, the Penyffordd Community council must be sure of your identity before complying with a subject access request. To confirm your identity, we need to see an official document with a photograph, such as a driving licence or a passport.

If you are making the request on behalf of another individual to access their information, we will need written consent from the individual to whom the data relates as well as your proof of identity.

If you have legal authorisation to act on behalf of an individual, such as if you act with power of attorney or as a litigation friend, you will need to provide a copy of that authorisation to evidence it.

We can refuse your request if it is manifestly unfounded or excessive, such as if it is repetitive. We will explain why we consider your request to be manifestly unfounded or excessive if we do refuse it.

Details of the person making the request	
Title:	
First name(s):	
Surname:	
Any other names that you have been known by	
Date of Birth:	
Address:	
Daytime telephone number:	
Email address:	

Are you requesting information about yourself?	
If Yes	Please go to section 4
If No	If you are making the request on behalf of another person you must enclose with the request a signed authority from them to do so. If you are making the application because the data subject lacks capacity to make the application in their own right please outline your authority to make the application in their stead (for example, Power of Attorney). You should enclose a copy of any evidence that you may have of that authority. The Council will contact you if further evidence is required. (please complete section 3)

Details of the Data Subject (if requesting information on behalf of someone else)	
Title:	
First name(s):	
Surname:	
Date of Birth:	
Address:	
Daytime telephone number:	
Email address:	
Relationship to Data Subject	

Describe the information you are requesting.
If you are only seeking certain records, it would be helpful for us to know which types of record you are seeking, any time period to cover, and if you would like to see only specific document(s). Please describe these below with as much detail as you can.

Declaration: I certify that the information given on this form is true and correct. Signed: Date:

Return Address : 3 Old Chester Road, Ewloe, Deeside, Flintshire, CH5 3RU

If as a result of the response to your request you are dissatisfied with the way we are using your personal information you should raise the matter with the Data Protection Officer who can be contacted via the address above. We will do everything we can to put the matter right if the council has not processed your data correctly. You also have a right to make a complaint about our handling of your personal data to the Information Commissioner's Office, whose web site is https://ico.org.uk/

We only use the information that you provide for us to process your request. We may need to share that you have made a request with other organisations if we hold information about you that they have supplied and we need to consult with those organisations regarding release of the information to you. Records of requests will be kept for 6 years after the closure of the request for operational, statistical and audit purposes.