St. Asaph City Council

CLOSED CIRCUIT TLEVISION (CCTV) POLICY AND CODE OF PRACTICE

CCTV POLICY

- The purpose of this policy is to regulate the management and use of the closed-circuit television (CCTV) systems operated by St. Asaph City Council.
- All x4 cameras are mounted on the outside of the Council Meeting Room building on Roe Pals, St. Asaph. The CCTV system is located in a secure, locked room within the Meeting Room Building.
- This CCTV scheme and policy is operated within the Information Commissioner's Code of Practice for CCTV 2008 and Surveillance Camera Code of Practice 2013 published by the Home Office.
- This policy will be subject to annual review, which will include a review in respect of the effectiveness and necessity of the system.
- The CCTV systems are owned wholly by the City Council.

OBJECTIVES OF THE CCTV SCHEME.

Along with a range of measures, the CCTV system will be used to:

- Reduce the fear of crime
- Deter crime and criminality
- Aid the detection of crime and the prosecution of offenders
- Reduce instances of nuisance and vandalism
- Promote a sense of safety to users of the building
- Provide safety and security to all vulnerable members of the community

STATEMENT OF INTENT

- The CCTV scheme will be registered with the Information Commissioner under the terms of Data Protection Act 1998 and will seek to comply with the requirements of the Data Protection Act and the Commissioner's Code of Practice, as well as the Surveillance Camera Code of Practice 2013 published by the Home Office.
- St. Asaph City Council will treat as data all CCTV recordings and relevant information.
- Cameras will be used to monitor all activities within the Council Meeting Room building in line with the objectives of the scheme.
- Static cameras are set as to not focus on private homes, gardens and other areas of private property.
- Materials of knowledge secured as a result of CCTV will not be released to the media, or used for any commercial purpose, or for the purpose of entertainment.

Recordings will only be released under the written authority from the Police, or in respect of a subject access request.

- The planning and design has endeavoured to ensure that the scheme will give maximum effectiveness and efficiency. It is not possible, however, to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
- Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the Council's CCTV.

OPERATION OF THE SYSTEM.

- The System will be administered by the City Clerk and other Council staff, in accordance with the principles and objectives expressed in the code.
- The CCTV system will be in operation 24 hours each day, for every day of the year.
- Systems will be checked on a monthly basis to ensure the system is operating effectively and in particular that the equipment is properly recording and that cameras are functional. The system will be regularly serviced and maintained by the Service Provider. Defects will be reported to the Servicing Company at the earliest convenient opportunity.

CONTROL OF SOFTWARE AND ACCESS TO THE SYSTEM.

- Access to the CCTV software will be strictly limited to authorised operators with a password.
- Operators must satisfy themselves that all persons viewing CCTV material will have a right to do so.
- The main control facilities must be kept secure.
- No information is downloaded or streamed to other systems, the data is automatically overwritten on a fortnightly basis. You can only access data for the last two weeks.

DIGITAL IMAGES: PROCEDURES

- Live and recorded materials may be viewed by authorised operators investigating an incident.
- Recorded material may be downloaded from the system in line with the objectives of the scheme.
- Images (stills and footage) may be viewed by the Police for the detection of crime.
- A record will be maintained of the release of images to the Police or other authorised applicants. A register will be available for this purpose.
- Viewing of images by the Police must be recorded in writing and in the log book. Requests by the Police are allowable under GDPR May 25th 2018.
- Should images be required as evidence, a digital copy may be released to the Police?
- The Police may require the City Council to retain images for possible use as evidence in the future. Such images will be securely stored until they are needed by the Police.
- Applications received from outside bodies to view or release images will be referred to the City Clerk. In these circumstances, images will normally be

released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee may be charged appropriate for subject access requests.

- Retention: Images will only be retained for only as long as these are required. The system automatically overwrites its data every fortnight.

BREACHES OF THE CODE (Including breaches of security).

- Any breach of the CCTV Code of Practice will be investigated by the City Clerk, in order for him/her to take any appropriate disciplinary action.

COMPLAINTS

- Any complaints about the CCTV system should be addressed to the City Clerk.

SUBJECT ACCESS AND FREEDOM OF INFORMATION

- The Data Protection Act (GDPR 25th May 2018) provides Data Subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV.
- Requests for Data Subject Access should be made in writing to the City Clerk.
- A request for Subject Access will be charged at £10, which is the maximum allowable under the GDPR May 25th 2018.
- A request under the Freedom of Information Act 2000 will be accepted, where such a request is appropriate.

CCTV CODE OF PRACTICE.

INTRODUCTION AND ACCOUNTABILITY.

The St. Asaph City Council has a comprehensive closed-circuit television (CCTV) surveillance system for the purpose of the prevention and detection of crime and the safety and welfare of staff and Meeting Room users.

The system is owned by St. Asaph City Council and images from the system are strictly controlled and monitored by authorised personnel.

This policy has been prepared from the standards set out in the Information Commissioner's CCTV Code of Practice 2008 and the Surveillance Camera Code of Practice 2013 published by the Home Office. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff and visitors to the Council Meeting Room Building and grounds and to ensure that it's operation is consistent with the obligations on the City Council imposed by the Data Protection Act 1998.

In line with the Home Office 12-point code of conduct the use of the system will:

- Always be for the purpose specified which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- Take into account its effect on individuals and their privacy.
- Have as much transparency as possible, including a published contact point for access to information and complaints.
- Have clear responsibility and accountability for all surveillance activities including images and information collected, held and used.
- Have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them.
- Have no more images and information stored than that which is strictly required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Be subject to appropriate security measures to safeguard against unauthorised access and use.
- Have effective review and audit mechanisms to ensure legal requirements, policies and standards are compiled with.
- 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, when used in pursuit of a legitimate aim.
- Be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.

OPERATION.

- The City Clerk is responsible for the operation of the CCTV system and for ensuring compliance with this policy. Any concerns in respect of the system's use or regarding compliance with this policy should be addressed to the City Clerk.

LOCATION

- This code of conduct applies to all CCTV systems operated by the City Council. Currently CCTV is present at the Council Meeting Room Building, Roe Plas, St. Asaph. It will also encompass all other CCTV images that, in due course, are added to the system.
- The system is operational and images are capable of being monitored by manually signing onto the system locally where the CCTV cameras are situated at any time of day, 24 hours a day throughout the whole year but only for the past two weeks (data is automatically overwritten ever two weeks).
- Images captured on camera will be recorded on the main CCTV server (locally on site in a secure location). Although every effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.
- For the purposes of the Data Protection Act 1998, the Data Controller is the St. Asaph City Council and the Council is legally responsible for the management and maintenance of the CCTV system.
- No unauthorised access to the system is allowed at any time. Normal access is strictly limited to authorised staff only.
- In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to access the CCTV system.
- Before granting access to the CCTV system, controllers must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitor's log, which shall include their name, department or organisation they represent, the person who granted authorisation for their visit (if applicable) and the start and finish times of their access to the CCTV system.
- It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with the procedures.
- Recorded images will only be reviewed with the authority for the City Clerk. Copies of digital images will only be made for the purpose of crime detection, evidence in relation to matters affecting safety, evidence for prosecutions, or where otherwise required by law.
- All staff involved in the operation of the CCTV system will, by training and access to this Policy, be made aware of the sensitivity of handling CCTV images and recordings.
- The City Clerk will ensure that all staff are fully briefed and trained in respect of all functions; operational and administrative, arising within the CCTV control operation. Training in the requirements of the Data Protection Act and this policy will also be provided.

RECORDINGS

- The system is supported by digital recording facilities which will function throughout operations in real time. As the images are recorded digitally, dates and times will also be recorded. Images will be cleared automatically every two weeks as it overwrites on a fortnightly basis.
- Unless required for evidential purposes or for the investigation of crime, recorded images will be retained for no longer than 14 days from the date of recording. However, the City Council recognises that, in accordance with the requirements of the Data Protection Act, no images should be retained for longer than is

necessary. Accordingly, some recorded images may be erased after a shorter period, for example where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded images. Digital images will be automatically erased after a set period, which will be no longer than 30 days.

- In the event of the digitally recorded image being required for evidence or the investigation of crime it will be retained for a period of time until it is no longer required for evidential purposes or any investigation into a crime has been completed.

DIGITAL RECORDING AND ACCESS PROCEDURES.

- Any/all disks containing images to remain the property of the City Council.
- Requests by persons for viewing or copying of disks or obtaining digital recordings will be usually be made by prior authority of the Police.
- Requests from the Police will arise in a number of ways, including:
    - Requests for a review of recordings in order to trace incidents that have been reported.
    - Immediate action relating to live incidents, e.g. immediate pursuit
    - For major incidents that occur when images may be recorded continuously
    - Individual Police Officers seeking to review recorded images.
- It is important that access to, and disclosing of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact, should the images be required for evidential Purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the policy reflect the Second and Seventh Data Protection Principles of the Data Protection Act 1998.
- All requests for access or disclosure will be recorded. The City Clerk will make decisions on access to recorded images by persons other than Police Officers. Requests by the Police for access to images will not normally be denied and can be made without the above authority, provided they are accompanied by a written request signed by a Police Officer who must indicate that the images are required for the purpose of a specific crime enquiry.
- If access or disclosure is denied, the reasons will be documented.
- If access to or disclosure of the images is allowed then the following will be documented:
    - The date and time at which access was allowed or the date on which disclosure was made
    - The reason for allowing access or disclosure.
    - The extent of the information to which access was allowed or which was disclosed
- Appropriate forms will be used to document routine disclosure to the Police.

PHOTOGRAPHS AND HARD COPY PRINTS

- Photographs and hard copy prints taken from digital images are subject to the same controls and principles of Data Protection as other data collected. They will be treated in the same was as digital images.

- At the end of their useful life all computer disks, still photographs and hard copy prints will be disposed of as confidential waste.
- This code of practice will be reviewed annually to assess its implementation and effectiveness.
- This code of practice is subject to annual review
- This code of Practice was approved by Full Council on May 9th 2018