|  |
| --- |
| [Installer to place their company logo here] |

**Surveillance Camera Code of Practice – Owner/Installer Points for Consideration**

| **Guiding Principle** | **Owner** | **Designer / Installation Company** |
| --- | --- | --- |
| 1. The 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.
 | To understand and document the requirements of the system, why it’s needed and how the images will be used. Collate adequate information to form an operational requirement.Any proposed extension to the original purposes for which a system was established should be subject to consultation before any decision is taken. | To fully understand the requirements of the customer, and the operational requirement of the CCTV system. To realise the requirements within the design of the system, and provide a detailed proposal and documented technical solution in order to confirm the installation complies with the operational requirement. To advise on positioning of cameras to help ensure the pressing need of the customer is met and the system is effective e.g. not positioning a camera where the view might be obscured by foliage etc. in the future.  |
| 1. 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.
 | Carry out appropriate consultation with those the system monitors prior to installation. Ensure the system required is proportional to the end needs. E.g. Audio recording and facial recognition systems would need significant additional justification.A Privacy Impact Assessment (PIA) should be undertaken as this will determine if any appropriate controls are required to ensure that a surveillance camera system takes into account the right of the citizen for privacy. It is good practice to make this available to members of the public e.g. on websites. | Technological solutions can be provided to ensure privacy is maintained, for example blocking out areas from view by cameras within programmed privacy zones. Guidance in redesigning a system to minimise the impact on individual’s privacy, e.g. repositioning camera locations could be given.  |
| 1. 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.
 | Provide adequate information for individuals to know the purpose of the CCTV scheme and who to contact in the event of a complaint or issue. Adequate signage as detailed within the Data Protection Act[[1]](#endnote-1) requirements can satisfy this need.Publish codes of practice and other policy documents such as PIAs, number of cameras in use on website so people can easily understand how your system is used. | Advice and guidance could be provided based on previous experience in installing similar systems. Assistance to source and install adequate CCTV data protection signage could also be provided as well as advice on where best to position it. |
| 1. There must be **clear responsibility and accountability** for all surveillance camera system activities including images and information collected, held and used.
 | Ensure that there are suitable individuals in place to govern and oversee the operation of the CCTV system. Clear written policy including individuals responsibilities are to be understood by all involved. Audit and review arrangements should be in place to ensure governance policies remain suitable, effective and sufficient.  | Guidance where required from experience within industry, advice concerning policy and audit/review arrangements could be provided.  |
| 1. **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.
 | Ensure that there are suitable rules, policies and procedures in place to govern and oversee the operation of the CCTV system. British Standard (BS)7958 gives best practice on the Management and Operation of CCTV.Ensure Security Industry Authority (SIA)[[2]](#endnote-2) licensing requirements are met if required. | Guidance could be given where required from experience within industry, advice concerning policy, procedures and audit/review arrangements based on own management systems or equivalent. |
| 1. **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.
 | Review Information Commissioner’s Office guidance for further advice. Determine the retention period for images depending on the requirements of the system. Request the designer allows for a system to automatically overwrite data after the retention period has expired, but will allow evidence to be exported when required for use by a law enforcement body. | Inform the client of the Information Commissioner’s Office guidance, and provide suitable equipment to meet the retention requirements within the design specification.The total storage requirements of the system could be calculated and clearly communicated to the customer. The design can also allow for a proportional additional amount. Options for future expansion must also be considered. |
| 1. **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.
 | Have in place suitable policies and arrangements to ensure requests and provision for disclosure of information is adequately dealt with.Review Information Commissioner’s Office documentation to understand the arrangements for subject access requests (Data Protection Act) and Freedom of Information Act[[3]](#endnote-3). | Provide guidance where relevant based on experience. Ensure systems and software specified can be easily used and understood by the owner, and allow different access levels to data and settings which are password protected. |
| 1. 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.
 | Ensure awareness of standards and legislation appropriate to the CCTV system; allow adequate resources to ensure compliance where necessary. Appoint a suitably competent designer/installer and check if they meet any relevant standards.A list of relevant standards is available on the Surveillance Camera Commissioner’s website[[4]](#endnote-4).  | Provide guidance and advice on relevant standards, and practical solutions to achieve compliance. The designer/ installer should have a proven track record of compliance and may also be certified to respected industry schemes – e.g. those offered by SSAIB and NSI[[5]](#endnote-5) or other inspectorates. Such companies will have access to and knowledge of the required standards and guidance.Inform end user of any standards you currently meet. |
| 1. Surveillance camera system images and information should be subject to **appropriate security measures** to safeguard against unauthorised access and use.
 | Ensure there is a clearly defined policy to control how images and information are stored, and who has access to them. Ensure adequate technical, organisational and physical security in place and guard against unauthorised use, access or disclosure of data. Review Information Commissioner’s Office documentation.  | Provide suitable design solutions for technical and physical security measures. Ensure Information Commissioner and owner requirements are included within any design proposals. |
| 1. 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.
 | Ensure resource is available and arrangements made to have regular audits of the CCTV system. These should be carried out at least annually, to ensure the scheme remains necessary, proportional and whether camera locations remain justified in meeting the stated purpose of the system. A summary of such a review available publicly as part of the transparency and accountability for the use and consequences of its operation. | Guidance and advice for carrying out audits, including the content of audit records. Assistance where required in carrying out the audits and implementing any changes to procedures.Subsequent assistance to introduce changes to CCTV system layout or architecture if findings of audit require such changes should be provided. |
| 1. 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.
 | Ensure requirements of law enforcement agencies which may require access to CCTV images are clearly understood. The operational requirement of the system must be understood and stated in the first instance. Suitable procedures and trained operators must be in place to effectively utilise any CCTV system. Ensure audit trails are retained regarding use of the system, viewing and exporting of images. Records of any exported data which is issued to third parties should be maintained. | Ensure advice and guidance is given to the end user regarding suitable proven technical solutions. Any design solutions should ensure images captured, retained and processed are of a suitable quality to meet the operational requirement of each element of the system. Integrity of images, associated meta data, and forensic integrity i.e. watermarking should also be considered.Any proposed system should also enable adequate audit trails to be documented. Suitable media which allows for the required retention periods whilst also allowing for effective export to law enforcement agencies when required could also form part of the design solution/installation. |
| 1. 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.**
 | Ensure regular assessments of data held within databases (e.g. where ANPR or facial recognition technology is used) which are referred to by a CCTV system take place. Such data should not be held for longer than necessary, and should only be used to fulfil the original purpose for which it was added to the database. Ensure adequate processes are in place to ensure these requirements are undertaken. | Provide advice based on previous experience of the most effective and suitable software systems to be used to record and manage such data. Ensure proposed systems are compatible with CCTV solution, and enable the end user to review, update and secure data as appropriate. |
| **Developed by ATEC Security in conjunction with the Surveillance Camera Commissioner** |

1. For information about the Data Protection Act or the Information Commissions Office(ICO) go to: [www.ico.org.uk](http://www.ico.org.uk) [↑](#endnote-ref-1)
2. For information about the Security Industry Authority go to: [www.sia.homeoffice.gov.uk](http://www.sia.homeoffice.gov.uk) [↑](#endnote-ref-2)
3. For information about the Protection of Freedoms Act go to: <http://www.legislation.gov.uk/ukpga/2000/36/contents> [↑](#endnote-ref-3)
4. For information about the Surveillance Camera Commissioner go to:  [www.gov.uk/government/organisations/surveillance-camera-commissioner](http://www.gov.uk/government/organisations/surveillance-camera-commissioner) [↑](#endnote-ref-4)
5. For information about inspectorates NSI or SSAIB go to:

a.       [www.nsi.org.uk](http://www.nsi.org.uk)

b.      [www.ssaib.org](http://www.ssaib.org) [↑](#endnote-ref-5)