St Albans City & District Council

COMMUNITY CCTV

CODE OF PRACTICE

ST ALBANS CITY & DISTRICT COUNCIL
CCTV CODE OF PRACTICE
REVIEWED OCT 2021

Contents

1. INTRODUCTION AND OBJECTIVES

1.1 Introduction

This Code of Practice has been written in accordance with the CCTV User Group Code of Practice, the Information Commissioner's CCTV Code of Practice and the National Surveillance Commissioner's CCTV Code of Practice.

This Code of Practice also applies to all CCTV cameras operated and managed by St Albans City and District Council for any other Local Authorities, agencies and bodies.

Glossary of Terminology

System Owner – **St Albans City and District Council**
District Council Offices
St Peters St
St Albans
Herts AL1 3JE
01727 866100

Ownership of the System with responsibility for overall responsibility for ensuring this Code of Practice is adhered to and that the System is properly maintained.

System Manager – **Neil Kieran**
St Albans City and District Council
District Council Offices
St Peters St
St Albans
Herts AL1 3JE
01727 819416
neil.kieran@stalbans.gov.uk

Day to day management of the System for and on behalf of the System Owner. Including data processing, management of the Code of Practice and performance of the System Operator with respect to monitoring and maintenance.

System Operator – **Videcom Security Ltd**
Videcom Security Ltd
Fordoun House,
Waltham Abbey,
Essex, EN9 1PF
01992 714604

Responsibility under contract to the System Owner, for the operation and maintenance of the System.

Data Controller	**St Albans City and District Council** **District Council Offices** **St Peters St** **St Albans** **Herts** **AL1 3JE** **01727 866100**

Overall responsibility for all data recorded by the CCTV System.

Data Processor	**Neil Kieran** **St Albans City and District Council** **District Council Offices** **St Peters St** **St Albans** **Herts AL1 3JE** **01727 819416** **neil.kieran@stalbans.gov.uk**

Responsible for the day-to-day management of all data recorded by the CCTV System.

Subject Access Request

This enables a person to request CCTV footage of themselves. Full details are contained in section 3.2 and Appendix A3.

Regulation of Investigatory Powers Act 2000

This is legislation that governs the use of CCTV to film persons secretly or as part of a planned operation by the Police and other enforcement agencies. Full details are contained in section 2.2.

1.2 Statement in respect of Human Rights Act 1998

The system owner has considered the obligations imposed by the above legislation and considers that the use of cameras in the locations as deployed is a necessary, proportionate and suitable tool to help prevent and detect crime and disorder.

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

1.3 Objectives of the system

The primary objective of the CCTV system is to protect and increase community safety, via the creation of a safe public environment for those living in and visiting the City and District. 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 promote community safety and to help reduce the fear of crime and disorder.
- To deter and detect incidents of anti-social behaviour, providing evidential material for criminal proceedings
- To assist with the economic development of the city and town centres.
- To assist local authorities with their enforcement and regulatory functions, providing evidential material for civil and criminal proceedings
- To assist with traffic management, providing information and co-operating with traffic flow projects
- To assist with other civil proceedings such as insurance claims

The need to assist with personal safety will over-ride any other requirements. For example, finding a missing child will take priority over criminal or anti-social events.

1.4 System Review

The system will be reviewed annually to ensure it remains necessary, proportionate, and effective. This review will also consider the location of cameras, types of transmission, image quality alternatives and future resource needs. The results of the review will be contained in the Annual CCTV Report.

2. STATEMENT OF PURPOSE AND PRINCIPLES

2.1 Purpose

The purpose of this document is to state how the Owner and System Manager intend to use the system to meet the objectives and principles outlined in Section 1.

2.2 General Principles of Operation

The system will be operated in accordance with this Code of Practice, The National Surveillance Camera Code of Practice and Guidance, and GDPR regulations at all times. Any request to use the system for covert surveillance will require the authorisation of the System Manager, or Control Room Manager if out of hours. This authorisation will only be given if the requesting agency has provided appropriately signed Regulation of Investigatory Powers Act 2000 documentation and demonstrated that the surveillance is both necessary and proportionate.

The system will be operated with due deference to the general right to respect for an individual and regard for their private and family life.

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

2.3 Copyright

Copyright and ownership of all material recorded by the system, will remain with the Data Controllers.

2.4 Monitoring and Recording Facilities

Fully functional cameras are connected to the Control Room, via fibre optic cable or via encrypted WIFI transmission. Other static cameras record to integral hard drives which are viewed in accordance with this Code of Practice.

2.5 Human Resources

All CCTV Operators are suitably registered with the Security Industry Association.

2.6 Processing and Handling of Recorded Material

No recorded material, whether digital, analogue, hard copy or otherwise will be released from the control centre unless it is in accordance with this Code of Practice.

2.7 Operator Procedures

CCTV Operators will follow standard operating procedures which comply with this Code of Practice.

2.8 Changes to the Code

All changes to this Code will be agreed by the Owners of the system.

3. PRIVACY AND DATA PROTECTION

3.1 General Data Protection Regulations (GDPR)

The operation of the system has been notified to the Office of the Information Commissioner in accordance with the current Data Protection Legislation.

All data will be processed in line with Article 5 of GDPR. It will be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

3.2 Request for Information – 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 System Manager and should be treated as a Subject Access Request.

Any person making such a request should use the form included at Appendix A3, including the fee of £10, and must be able to provide sufficient information to prove their identity and to enable the data to be located.

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

In accordance with the GDPR, personal data processed for the prevention or detection 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.

A request from an individual for footage of 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.

4. ACCOUNTABILITY AND PUBLIC INFORMATION

4.1 The Public

Access to the CCTV control room is restricted in accordance with this Code of Practice.

A member of the public wishing to register a complaint with regard to the system should contact the System Manager at the address provided within this Code. All complaints will be dealt with in accordance with the relevant Council's complaints procedure.

4.2 System Manager

As detailed on the front page of this Code, the Principal Community Protection Officer, employed by St Albans City and District Council, is the System Manager.

The System Manager, in conjunction with the Control Room Manager (employed by the contractor providing the CCTV operators) will have day to day responsibility for the system. This includes ensuring this Code of Practice is adhered to.

4.3 Public Information

This Code will be made available on the Council's website and upon request to the System Manager.

Signage is erected in the locality where cameras are deployed. An example is included at Appendix A5.

5. ASSESSMENT OF THE SYSTEM

5.1 Evaluation

The operation of 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 1.

5.2 CCTV Monitoring Group

The CCTV Monitoring Group meets every two months to consider Police hot spots, deployment of temporary CCTV, usage of the CCTV System and any new proposed initiatives and ideas. This group consists of the System Manager, Control Room Manager, the Police, St Albans Business Against Crime, Harpenden Town Council, and others as required by operational needs.

5.3 Annual Report

An annual report will be produced, which will give an overview of usage for the previous year, details of the annual system review, incidents of note, statistics relating to usage and details of planned upgrades and developments.

This report will initially be submitted to the Lead Councillor for community engagement and support services, and to the Chair of the Scrutiny Committee.

The Annual Report will be published on the Council's website.

6 HUMAN RESOURCES

6.1 Staffing of the Control Room

All staff operating cameras in the control room will have a valid Security Industry Association (SIA) Public Space Surveillance Licence. Operators will also be issued with a copy of this Code of Practice and will be conversant with all contents.

6.2 Discipline

Every individual with responsibility under this code, and who has any involvement with the system is subject to this code and will sign the declaration of confidentiality attached at Appendix A4. Breach of this Code will be treated as a serious disciplinary matter.

7. CONTROL AND OPERATION OF CAMERAS

7.1 Guiding Principles

All persons operating the cameras will act with utmost probity at all times.

Cameras will not be used to look into private residential property unless pursuing a suspect or an appropriate Regulation of Investigatory Powers Act authorisation is in place.

Camera operators will not exercise any prejudice, with operators being required to justify their interest in, or recording of, any particular group of individuals to the System Manager.

7.2 Operation of the System by the Police

Only in extreme circumstances and upon the written request of a Superintendent or above will the Police be able to direct use of a part of the system. This will need the written approval of the Head of Department, with such approval designating the specific Police staff to who this power has been granted, for what purpose and for what timescale.

In the event of such a request being granted, the control room will continue to be staffed and operated by those personnel authorised to do so and who fall within the terms of this code.

In very extreme circumstances a request may be made by the Police to take total control of the system in its entirety, including the staffing of the monitoring room and personal control of the associated equipment, to the exclusion of the System Manager. Any such request must be made in writing by an Assistant Chief Constable or above to the System Manager, who will need to obtain the written approval of the Council's Chief Executive. Such approval will designate the specific Police staff to whom this power has been granted, for what purpose and for what timescale.

7.3 Maintenance of the System

To ensure that the system continues to provide footage of sufficient evidential quality, the Owner will ensure a maintenance agreement is always in place.

8.SECURITY ARRANGEMENTS OF THE MONITORING ROOM

8.1 Security Arrangements

The CCTV Control Room is a secure environment, controlled via an electronic access scheme. Only persons authorised by the System Manager will be allowed access.

8.2 Public Access

This will only be granted by the System Manager. Authorised visitors will be supervised at all times and will be required to sign the declaration of confidentiality and provide their full name and address, as detailed on 8.3 below.

8.3 Declaration of Confidentiality

All visitors to the CCTV Control Room will be required to sign the visitors' book which contains the following declaration of confidentiality:

In signing this visitors' book, I acknowledge that any footage disclosed to me is only to be used for the purpose for which it is disclosed and for no other reason, within the explicit written permission of the System Manager. I also acknowledge that personal details of those operating the system must not be divulged and I agree not to divulge any information obtained, overheard or seen during my visit to the CCTV Control Room.

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 the system; this specifically includes images recorded digitally or on other media including still prints.

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.

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 material is treated strictly in accordance with this Code of Practice until the final destruction of the material.

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

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.

9.2 National Standard for release of data to a third party

Requests from the Police for footage for the prevention and/or detection of crime and disorder will be submitted to the Control Room Manager. All other requests will need the approval of the System Manager. The System Manager will ensure the principles contained within the National Standard (Appendix A2), are followed at all times.

In complying with the National Standard it is intended, 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 this Code.
- Access to recorded material will only take place in accordance with the National Standard and this Code.

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 System Manager and will be recorded.

It may be beneficial to make use of recorded material for training of those operating the System. This will only take place with the permission of the System Manager.

9.3 Footage and Recorded Material – retention

Images recorded by full function cameras that provide live footage to the control room are retained on hard drives for 28 days. Images recorded by static cameras onto hard drives are in situ for 14 days. After these time periods the footage is automatically erased.

When footage is released as recorded material a master copy is made and retained securely by the CCTV Control Room. This is the retained for 7 years after which it is securely destroyed.

9.4 Register and Release of Recorded Material

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

9.5 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.

APPENDIX A1 KEY PERSONNEL AND RESPONSIBILITIES

System Manager – **Neil Kieran**
St Albans City and District Council
District Council Offices
St Peters St
St Albans
Herts AL1 3JE
01727819416 **neil.kieran@stalbans.gov.uk**

Day to day management of the System for and on behalf of the System Owner. Including, data processing, management of the Code of Practice and performance of the System Operator with respect to monitoring and maintenance.

System Operator – **Videcom Security Ltd**
Videcom Security Ltd
Fordoun House,
Waltham Abbey,
Essex, EN9 1PF
01992 714604

Responsibility under contract to the System Owner, for the operation and maintenance of the System.

Control Room Manager **Jason Farmer-Ward**
Videcom Security Ltd
Videcom Security Ltd
Fordoun House,
Waltham Abbey,
Essex, EN9 1PF
01992 714604

Employed by the System Operator to manage the operation and maintenance of the system.

APPENDIX A2 NATIONAL STANDARD FOR RELEASE OF DATA TO THIRD PARTIES

General Policy

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 Control Room Manager – all other requests for footage will be dealt with by the System Manager. Day to day responsibility for the operation of the CCTV system lies with the System Manager.

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, 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).

v) Identification of witnesses

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

i) Police (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, Ministry of Defence Police, Military Police, etc. (Special arrangements may be put in place in response to local requirements.)

(2) Aside from criminal investigation, 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 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 controller shall ensure that:
i) The request does not contravene and that compliance with the request would not breach current relevant legislation, (e.g., Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.).

ii) Any legislative requirements have been complied with (e.g., the requirements of the Data Protection Act 1998).

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’ (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 to 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.

ii) If the material is to be released under the auspices of ‘public well being, health or safety’, written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV 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 of 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 legislation individual access to personal data, of which that individual is the data subject, must be permitted providing:

i) The request is made in writing.

ii) A specified fee is paid for each search.

iii) A data controller is supplied with sufficient information to satisfy 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 those circumstances it is suggested that within one hour of accuracy would be reasonable requirement).

v) The person making the request is only shown information relevant to that particular search and which contains personal data of hi/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 contained within the Data Protection legislation, the data controller should be satisfied that the data is:

i) Not currently and as far as can be reasonably ascertained, not likely to become part of a ‘live’ criminal investigation.

ii) Not currently and as far as can be reasonably ascertained, not likely to become relevant to civil proceedings.

iii) Not the subject of a complaint or dispute which has not been actioned
iv) The original data and that 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 responsible person acting on their behalf).

c) The viewing should take place in a separate room and not in the control room or monitoring area. Only data relevant to the request to be shown.

d) It must not be possible to identify any other individual from the information being shown (any such information will be blanked out, either by means of electronic screening or manual editing on the monitor screen.

e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

Note: The Information Commissioners 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 on its use.

ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g., specific identities/data that must not be revealed.

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 legislation 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 publicised 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 assurance that the broadcasters would mask 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 to the requirements of the Information Commissioners in this respect, detailed in her Code of Practice summarised above.

6. Principles

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 of Practice for the system.

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

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

APPENDIX A3

Subject Access Request Form

ST ALBANS CITY & DISTRICT COUNCIL CCTV SURVEILLANCE SYSTEM

How to Apply For Access To Information Held On the CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. The Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

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

The Council's Rights

The Council may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

Fee

A fee of £10 is payable for each access request.

THE APPLICATION FORM: (N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)

When you have completed and checked this form, take or send it together with the required TWO identification documents, photograph and fee to: The Principal Community Protection Officer, St Albans City & District Council, St Peters St, St Albans, Herts, AL1 3JE

ST ALBANS CITY & DISTRICT COUNCIL CCTV SURVEILLANCE SYSTEM

SECTION 1 About Yourself

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

PLEASE USE BLOCK LETTERS

Title **(tick box as appropriate)**	***Mr***		***Mrs***		***Miss***		***Ms***	
Other title **(e.g., Dr., Rev., etc.)**								
Surname/family name								
First names								
Maiden name/former names								
Sex **(tick box)**	***Male***				***Female***			
Height								
Date of Birth								
Place of Birth	***Town***							
	County							

Your Current Home Address	
	Post Code
A telephone number will be helpful	***Tel. No.***

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

Previous address(es)		
Dates of occupancy	***From:***	***To:***
Dates of occupancy	***From:***	***To:***

ST ALBANS CITY & DISTRICT COUNCIL CCTV SYSTEM

SECTION 2 Proof of Identity

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

For example: a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address.

Also, a recent, full face photograph of yourself.

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

SECTION 3 Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Please tick the box that applies.

Do you wish to:

(a) View the information and receive a permanent copy ☐

(b) Only view the information ☐

SECTION 4 To Help us Find the Information

If the information you have requested refers to a specific offence or incident, please complete this Section.

Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.

If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.

Were you: **(tick box below)**

A person reporting an offence or incident	
Victim of an offence	
A witness to an offence or incident	

Other – please explain	

Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident	

SECTION 4 Declaration

DECLARATION ***(to be signed by the applicant)***

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

Signed by

Date

APPENDIX A4 DECLARATION OF CONFIDENTIALITY

St Albans City & District Council

CONTRACTOR CONFIDENTIALITY & AGREEMENT WITH CODE OF PRACTICE

This **AGREEMENT** is made on

BETWEEN

St Albans City & District Council ("the Principal Client")

AND

The Contractor's employee ("The Service Provider")

In consideration of the Principal Client engaging the Service Provider to provide security services ("The Services"), the Service Provider agrees and confirms that:

1.0 In the course of providing the Services to the Principal Client, the Service Provider will receive and acquire confidential information which is the property of the Principal Client or it's customers, or associated entities.

2.0 The Service provider will, during and after its service to the Principal Client, take all reasonable steps to keep confidential all information which is disclosed to or obtained by the Service Provider as a result of or during the course of its service to the Principal Client

3.0 During and after its service to the Principal Client, the Service Provider will not:

3.1 disclose to any person confidential information relating to the business or affairs of the Principal Client, its customers or associated entities unless specifically authorised to do so by the Principal Client in writing

3.2 other than to the extent which is necessary to enable the Service Provider to perform its duties:

3.2.1 make extracts from, copy or otherwise duplicate confidential information;

3.2.2 make adaptations of confidential information;

3.2.3 make use of confidential information for private purposes, or in any manner which may, or is calculated to cause injury or loss to the Principal Client, its customers or associated entities;

3.2.4 other than for the benefit of the Principal Client, make notes, documents, working papers or memorandum relating to any matter within the scope of the business of the Principal Client or concerning any of its dealings or affairs.

4.0 Clauses 2.0 and 3.0 shall continue to apply despite the termination or cessation of the Service Provider service by either the Principal Client or the Service Provider.

5.0 I agree to abide by the Principal Client's Code of Practice as issued and updated.

6.0 Without limiting the generality of the above, for the purposes of this clause, confidential information means and includes any information relating to the business and activity of the Principal Client or it's customers or it's associate entities including but not limited to intellectual property financial information and other commercially valuable information in whatever form and all other information provided to the Service Provider which is either labeled or expressed to be confidential or given to the Service Provider in circumstances where one would expect the information to be confidential to the Principal Client, or it's customers or it's associate entities, but excluding any matter that has become public knowledge or part of the public domain.

The Service Provider undertakes to comply with the above obligations and conditions as required by the Principal Client and as stated above to protect the confidential information of the Principal Client and all relevant compliance requirements.

Name Signature Date

APPENDIX A5 EXAMPLE OF SIGNAGE