CLOSE CIRCUIT TELEVISION (CCTV) POLICY

TOTNES TOWN COUNCIL
OCTOBER 2018
REVIEW DATE: XXXX

CONTENTS

1. Introduction

1.1 The use of Closed Circuit Television is viewed by Totnes Town Council as a key element in its promotion of security and safety. CCTV cameras are installed on the Guildhall and Council Offices front door.

1.2 The Town Council will have due regard to the Data Protection Act 1998, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998

1.3 This policy sets out to ensure the effective use of CCTV to prevent crime, identify the perpetrators of crime, enhance community safety and reduce the fear of crime. Its aim is to ensure that all residents, visitors and businesses have the confidence to undertake their activities during the day or night without fear and with confidence in their safety and the security of the environment.

1.4 Ownership of recorded material remains at all times the property of Totnes Town Council.

1.5 The CCTV cameras are operated from the Town Clerk's office in the Council building and images are recorded digitally.

1.6 The Committee responsible for monitoring and running the effectiveness of the system will be the Council Matters Committee.

2. Purpose Statement

2.1 The system is intended to provide an increased level of security at the Town Council and historic Guildhall.

2.2 The CCTV system will be used to respond to the following key objectives, which will be subject to annual assessment:

- To detect, prevent or reduce the incidence of crime
- To prevent and respond effectively to all forms of harassment and public disorder
- To create a safer community
- To gather evidence by a fair and accountable method

2.3 In this respect, cameras have been sited so that their primary view is of public areas.

2.4 Respect for privacy is an important consideration and the system will not be used to monitor individuals undertaking day to day activities in areas under surveillance.

2.5 To ensure that the public is aware that they are entering an area where a scheme is in operation, signs have been placed at the entrance to all areas covered. All signs will be fit for purpose and careful consideration will be given to placement, size, opportunity to view etc.

2.6 The signs will indicate that CCTV cameras are operating and will be displayed at the perimeter of the area covered by the scheme.

2.7 The signs will identify the owner by name and provide a daytime contact telephone number.

3. Ownership Details

3.1 For the purposes of the Data Protection Act 1998 the beneficial owner of the system is:

Totnes Town Council
The Guildhall Offices
5 Ramparts Walk
Totnes
TQ9 5QH

3.2 The system is registered with the Information Commissioner under registration Z7595350.

4. Data Protection Implications

4.1 The scheme is registered under the Data Protection Act and Totnes Town Council undertakes to co-operate at all times with the Information Commissioner.

4.2 Data will be held and stored only for the purpose set out in this policy and in accordance with its provisions.

4.3 Totnes Town Council is the Data Controller and has designated authority to the Town Clerk for the day to day running of the system. In their absence, the Deputy Clerk will assume authority.

5. The Digital Recorders and the Recording of Images

5.1 All images are recorded onto digital recorders in the Council office.

5.2 All CCTV equipment will be kept in good working order and be serviced according to manufacturer's recommendations.

5.3 When a fault develops on the CCTV system, it shall be reported immediately to the service engineer.

5.4 The system time clock and/or recording device time clocks shall be checked on a quarterly basis and set to the correct hour with reference to a reliable time signal e.g. Speaking Clock (123).

5.5 All CCTV equipment shall be kept in the Council office and password protected to prevent unauthorized or unlawful processing of personal data and against accidental loss, damage or destruction of personal data.

5.6 Any data held for evidential purposes will be kept away from other personal data in a secure location.

5.7 No unauthorised copies will be made of any personal data except with the permission of the Data Controller who shall record the reason and ensure that all copies are numbered and that they are only disclosed to authorised parties. The Data Controller will also ensure such personal data is not kept for longer than is necessary and is destroyed as if it were an original recording.

5.8 Digital recordings will be retained for no longer than 31 days, unless they are required to be used as evidence in any legal proceedings. After 31 days, the images will be deleted. Recorded material will be used only for purposes defined in this policy.

5.9 Access to recorded material will only be permitted as defined in this policy.

5.10 Recorded material will not be sold or used for commercial purposes or the provision of entertainment.

5.11 Ownership of recorded material and copyright in recorded material is that of Totnes Town Council.

6. Recorded Images as Evidence

6.1 The Police will apply verbally for access, in accordance with an agreement made with Totnes Town Council, where the Police reasonably believe that access to the recorded images is necessary for the investigation and detection of a particular offence or offences or the prevention of crime.

6.2 The Police may obtain access under the provisions of the Police and Criminal Evidence Act 1984.

6.3 Recorded material resulting from the operation of the system will normally only be made available to the Police for criminal prosecution purposes.

6.4 On occasion, specific requests may be received from other organisations with prosecution powers such as HM Customs and Excise, South Hams District Council, the Health and Safety Executive and Trading Standards. In the event that the evidence is required in connection with a prosecution that will assist in the achievement of the key objectives of the system, the evidence will be supplied if agreed by the owners and after consultation with the Police. Any evidence supplied will be subject to an undertaking that it will only be used strictly in accordance with this policy and for the reasons for which it has been supplied.

6.5 Since recorded material may be admitted in evidence, it must be of good quality, accurate in content and treated according to defined procedures to provide continuity of evidence and to avoid contamination of the evidence.

6.6 Appropriate security measures will be taken against unauthorised access to, alteration, disclosure, destruction or accidental loss of recorded material.

6.7 USB drives/DVD discs required for evidential purposes will be treated as exhibits and will be retained and stored according to procedures agreed with the Police, as follows:

• An original exhibited Master USB/DVD will be produced only on receipt of a written request from the Police (please see Appendix 2)
• The Master USB/DVD will be retained under secure storage by the Data Controller and secured with a tamper proof label
• An exhibited working copy will also be produced if required
• The Master USB/DVD will be given a unique reference number (comprising date, in dd/mm/yyyy format, together with the associated crime reference number) which shall be indelibly marked on the disc
• A register will be maintained in which a record of the Master UBBs/DVDs held by the Data Controller will be logged. The register will be securely stored by the Data Controller in the Town Council's offices at all times unless it is required for production in court
• The Data Controller will log the issue of a working copy and the authorised police officer receiving the USB/DVD will sign for it

• If necessary, the Town Clerk will provide the Police with statements required for evidential purposes

6.8 Third party access to recorded images may be permitted in connection with civil disputes by court order or be extended to lawyers acting for defendants or victims in connection with criminal proceedings.

6.9 No other access will be allowed unless approved by the owners and for reasons that fall within the purposes and objectives of the system and in accordance with this policy and the Data Protection Act.

7. Control and Operation of Cameras

7.1 Only those staff with direct responsibility for using the equipment shall have access to the operating controls.

7.2 All use of the cameras shall accord with the purposes and key objectives of the system and shall comply with this policy.

7.3 Cameras shall not be used to look into private property. Where appropriate operational procedures and technological measures will be adopted to impose restraints upon the use of cameras in connection with private premises.

7.4 The system will only be viewed/operated by trained operators. This will apply to staff from the Devon and Cornwall Constabulary and staff employed by Totnes Town Council. The Data Controller will maintain a list of all trained personnel.

8. Accountability

8.1 In accordance with the Code of Practice and the Data Subject Access Rights of The Data Protection Act 1998, anyone wishing to acquire a copy of the policy or to request further information with regard to accessing the recorded data under the Data Protection Act 1998 should be directed to contact the Data Controller in writing.

8.2 Copies of this policy will be made available by:

The Data Controller, The Guildhall Offices, 5 Ramparts Walk, Totnes TQ9 5QH

<u>Subject Access Requests</u>

9. Access to Personal Data under the Data Protection Act

9.1 Under the terms of data protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:

• The request is made in writing (please see Appendix 1)
• A specified fee is paid for each individual search
• The Data Controller is supplied with sufficient information to satisfy them as to the identity of the person making the request

• 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 is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement)
• The person making the request is only shown information relevant to that particular search and which contains personal data of her/himself only, unless all other individuals who may be identified from the same information have consented to the disclosure
• 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)

9.2 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 merit.

9.3 In addition to the principles contained within the data protection legislation, the Data Controller/Town Clerk should be satisfied that the data is:

• Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation
• Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings
• Not the subject of a complaint or dispute which has not been actioned
• The original data and that the audit trail has been maintained
• Not removed or copied without proper authority
• For individual disclosure only (i.e. to be disclosed to a named subject)

9.4 Upon receipt of a bona fide request to verify the existence of relevant data and payment of the appropriate fee (currently £10.00), the Town Clerk will ensure:

• No undue obstruction of any third party investigation to verify existence of data
• The retention of data which may be relevant to a request
• That there is no connection with any existing data held by the Police in connection with the same investigation

9.5 Any member of staff receiving a subject access request must note the name and address of the person making the request in order that the appropriate form may be sent to them. The details should then be passed without delay to the Data Controller or Deputy Clerk.

9.6 The Data Controller, or Deputy Clerk, will then send by first class mail a subject access request application form.

9.7 The Data Controller will only deal with subject access requests that are in writing and that are accompanied by a fee of £10.00.

9.8 On receipt of the completed form and the fee, the Data Controller will assess if there is sufficient information to locate the data subject contained within the reply. If not he/she will, without delay, write to the Data Subject and request the necessary information. If a reply is not received within 7 working days he/she shall disregard the request and record the reason for so doing.

9.9 On receipt of a subject access request and the required fee, the Data Controller shall process the request within 31 days.

9.10 Only the Data Controller or Deputy Clerk will attempt to locate the images and be responsible for decisions regarding disclosure.

9.11 The Data Controller or Deputy Clerk will decide if disclosing images will identify third parties and whether those images are held under a duty of confidence.

9.12 Any images so held will have the images of third parties blurred out or disguised.

9.13 Data Subjects may be asked if they merely wish to view their data, otherwise they will be provided with a copy of the CCTV data in standard USB/DVD format.

9.14 All third party viewings will take place in a private area away from the CCTV recording and monitoring facility.

9.15 If subject access is denied, the Data Controller will record the details of the refusal and inform the enquirer of the decision in writing.

9.16 If the Data Controller receives a request to cease processing personal data on the grounds that it is likely to cause unwarranted damage or distress, he must respond in writing to the individual within 21 days and state whether or not he will comply with the request, giving reasons for the decision.

9.17 The Data Controller will maintain a record of all such requests and the resultant decision.

10. Primary Request to View Data

10.1 Primary requests (i.e. those from law enforcement agencies) to view data generated by the CCTV system are likely to be made by third parties for any one or more of the following purposes:

• Providing evidence in criminal proceedings (Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996)
• Providing evidence for civil proceedings or tribunals
• The investigation and detection of crime
• Identification of witnesses

10.2 Third parties will be required to show adequate grounds for disclosure of data within the above criteria, this may include, but is not limited to:

• Police
• Statutory authorities with powers to prosecute
• Solicitors
• Plaintiffs in civil proceedings
• Accused persons or defendants in criminal proceedings

10.3 All primary requests will be recorded in a spreadsheet administered by the Town Clerk.

11. Secondary Request to View Data

11.1 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:

• The request does not contravene, and that compliance with the request would not breach, current relevant legislation (eg. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc)

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

• Due regard has been taken of any known case law (current or past) which may be relevant (eg. R v Brentwood BC ex p. Peck)

• The request would pass a test of 'disclosure in the public interest'

11.2 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:

• 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 System Code of Practice.

• 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 System Code of Practice.

12. The Media

12.1 Where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident will be taken into account. In all cases of media disclosures for the purposes of this clause the police authority will have the sole discretion of disclosure.

13. Training

13.1 All staff that handle or manage personal data derived from the CCTV system will receive appropriate training in the following fields:

1. Recognition of a subject access request

2. Recognition of a request to prevent processing likely to cause a Data Subject unwarranted

damage or to prevent automated decision taking

3. The use of appropriate forms

4. What action to take on receipt of a request

5. How enquirers might be provided with a copy of this policy

6. How enquirers might make a complaint about the CCTV system either to the owner or Information Commissioner

14. Complaints

14.1 Any use of the CCTV system or materials produced which is outside the policy and is inconsistent with the objectives of the system will be considered gross misconduct.

14.2 Misuse of the system will not be tolerated; continuing public support is vital. Any person found operating outside this policy without good and reasonable course will be dealt with under the Council's disciplinary system. If any breach constitutes an offence under criminal or civil law then court proceedings may be taken.

14.3 Any complaint concerning misuse of the system will be treated seriously and investigated by the Town Clerk. The Town Clerk or Deputy Clerk will ensure that every complaint is acknowledged in writing within seven working days, which will include advice to the complainant of the enquiry procedure to be undertaken.

14.4 Where appropriate the Police will be asked to investigate any matter recorded by the CCTV system which is deemed to be of a criminal nature.

15. Major incidents

15.1 In the event of a major incident arising, such as serious public disorder, bomb threats/explosions or serious fires, the Police will be given authority to supervise the CCTV. Such authority will be given by the Town Clerk or Deputy Clerk verbally or in writing under the constraints of The Regulation of Investigatory Powers Act 2000.

Appendix 1

Totnes Town Council CCTV

Subject Access Request

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. Totnes Town 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)

Totnes Town Council's Rights

Totnes Town 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

• Giving you the information may be likely to prejudice any of these purposes

Fee

A fee of £10.00 is payable for each access request, which must be in pounds sterling. Cheques should be made payable to 'Totnes Town Council'.

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

Section 1

Asks you to give information about yourself that will help the Council to confirm your identity. Totnes Town Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2

Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full face photograph of you.

Section 3

You must sign the declaration. When you have completed and checked this form, take or send it together with the required TWO identification documents, photograph and fee to:

Data Controller, Totnes Town Council, The Guildhall Offices, 5 Ramparts Walk, Totnes TQ9 5QH.

Totnes Town Council CCTV

Subject Access Request

This form is used to confirm the identity of the Data Subject, the identity and authority of the applicant (where applicable) and to assist in locating personal data relating to the Data Subject.

Please complete it and send it to the address at the end of the form. If you need any help please call 01803 862147.

SECTION 1

Data Subject's full name……..

Date of Birth……..

Address

……

……

……

……Post code……

Telephone No……

E-mail address……..

(a) Are you the Data Subject? Yes / No

If you answered 'Yes', go straight to Question 3. Otherwise, please provide the information below.

Your full name……

Address

……..

……..

……..

……Post code……..

Telephone No……..

(b) If you are NOT the Data Subject, state your relationship to them.

What is your relationship to the Data Subject?.....

(c) If you are NOT the Data Subject, describe your entitlement to receive details of their personal data, and the written authority enclosed (e.g. from the Data Subject) which supports this entitlement.

Why are you entitled to their Personal Data?.....

.....

What written authority have you
enclosed?.....

.....

Our search for information relating to the Data Subject will be based on the information provided below.

CCTV footage (please tick)……

Date and time of incident when you believe image was captured (within 1 hour)……

……

Location of incident……

Brief description of incident……..

……

Brief description of the clothing worn by the Data Subject at time of incident……

……

SECTION 2

We must see the original documents and we cannot accept photocopies. Note that Totnes Town Council will return all documents as soon as possible via recorded delivery. If you deliver your documents in person we will return them to you after verification - please call 01803 862147 for further information.

(a) You must **confirm the Data Subject's identity** by sending one of the documents listed below.

Please tick to indicate which documents you have enclosed.

i) Full Valid Driving licence issued by a member state of the EC/EEA……

ii) Birth Certificate or Certificate of Registry of Birth or Adoption certificate……..

iii) Full Valid Current Passport or ID Card issued by a member state of the EC/EEA or Travel Documents issued by the Home Office or Certificate of Naturalisation or Registration or Home Office Standard Acknowledgement Letter (SAL)……

If the Data Subject's name is now different from that shown on the document you submit to confirm his/her identity, you must also supply original documentary evidence to confirm the Data Subject's change of name e.g Marriage Certificate, Decree Absolute or Decree Nisi papers, Deed Poll or Statutory Declaration.

(b) You must also **confirm the Data Subject's address** by sending us one of the documents listed below.

Please tick to indicate which documents you have enclosed.

i) Gas, electricity, water or telephone bill in the Data Subject's name for the last quarter……

ii) Council Tax demand in the Data Subject's name for the last quarter……..

iii) Bank, building society or credit card statement in the Data Subject's name for the last quarter….

iv) Letter to Data Subject from solicitor/social worker probation officer in the last quarter……

(c) You must also send us **a recent passport sized photograph of the Data Subject.**

SECTION 3

In exercise of the right granted to me under the terms of the Data Protection Act 1998, I request that you provide me with a copy of the personal data about the Data Subject which you process for the purposes I have indicated overleaf.

I confirm that this is all of the personal data to which I am requesting access. I also confirm that I am either the Data Subject, or am acting on their behalf.

Signed……

Print name……

Date……

Make sure you have:

(a) completed this form

(b) signed the declaration above

(c) enclosed originals of identification documents

Send to: **Data Controller, Totnes Town Council, The Guildhall Offices, 5 Ramparts Walk, Totnes TQ9 5QH.**

We recommend that you send your form and documents by a secure method e.g. Recorded Delivery.

SECTION 4 – FOR OFFICIAL USE ONLY

Application checked and legible? …… Date Application received……

Identification documents checked?.....

Details of Document Produced…….

……

Documents Returned?.....

Member of staff completing this section

Name ……..Location…….

Signature ……Date……

Request - Granted / Denied

If Granted, please complete the following section:

Camera Number……

Operators Details……..

Video Print Log Reference Number……..

Master DVD Reference Number…….

Date of Issue……...

Subject Access Signature or Proof of delivery address……..

……

CCTV Managers Name……

CCTV Managers Signature……

Comments……

……

……

Before returning this form

• Have you completed ALL Sections in this form?

Please check:

• Have you enclosed TWO identification documents?

• Have you signed and dated the form?

• Have you enclosed the £10.00 (ten pound) fee?

Further Information: These notes are only a guide. The law is set out in the Data Protection Act, 1998.

Further information and advice may be obtained from: **The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel. (01625) 545745**

Appendix 2

Totnes Town Council
The Guildhall Offices
5 Ramparts Walk
Totnes
TQ9 5QH

Date:
Telephone:
Direct Dial:

My Ref:

Ask for: Extension:

Dear Sirs,

Authority to view / request copy of CCTV digital hard drives.

In accordance with Totnes Town Council's CCTV Policy, please permit ……..to view the digital hard drives following a recent incident.

a. OIS log Number and Date or Crime Reference Number …….

OR

b. Which occurred at about ……(time/date/location)

i. I also ask that you retain the original exhibited master copy DVD(s) and produce an exhibited working copy with a supporting statement of evidence if required. (The Master DVD(s) must be retained under secure storage until the Police Liaison Officer confirms criminal proceedings have concluded).

ii. IN RELATION TO MAJOR INCIDENTS ONLY – that you produce a master and working copy DVD(s) from the digital hard drive and hand both to the officer against signature.

Yours faithfully

…….. **……**
Requesting Officer **(Printed surname)**

Time…… …….