Buckingham Town Council Provision of CCTV Policy	**Date Agreed: 20th Sept 2021** **Minute Number: 364.1/21** **Prepared by:** Lee Phillips **Version: 1.1**

1 Introduction

1.1 This policy is to set out Buckingham Town Council's procedures regarding the management of the mobile surveillance camera(s). Buckingham Town Council (BTC) in Partnership with Thames Valley Police (TVP) has obtained a mobile CCTV system for use around the town. The system has been established to help prevent and detect crime in Buckingham and will not be used for any other purposes.

2 Twelve Guiding Principles

2.1 The system will be operated using the following 12 guiding principles contained in the Surveillance Camera Code of Practice (The Home Office, June 2013). These are:

(a) 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.

(b) 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.

(c) There must be as much 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.

(d) There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

(e) Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all partner organisations.

(f) 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.

(g) 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.

(h) 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.

(i) Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

(j) 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.

(k) 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.

(l) 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.

3 Retaining recorded material

3.1 Recorded material is stored on a hard drive within the camera and is only accessible by a secure internet connection via authorised computers.

3.2 The hard drive automatically deletes the recorded images as the drive becomes full, this occurs after approximately one month.

4 Disclosure of recorded material and the Data Protection Act

4.1 The disclosure of images to law enforcement agencies where a crime needs to be investigated will always be permitted.

4.2 Images will not be released directly to the media except for identification purposes, and only on the advice of a law enforcement agency.

4.3 Images will not be put on the Internet for entertainment purposes.

4.4 BTC has the discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights.

4.5 BTC may disclose only images if there is a legitimate reason for the request to do so, for example where an incident occurs and the person in the footage wants to proceed with an insurance claim, in which case may allow the use of the footage at its discretion.

4.6 Individuals whose images are recorded have the right to view the images of themselves and may be provided with a copy of those images, which must be provided within 40 calendar days of receiving such a request. BTC may charge a fee of £10 (or up to any such maximum set by Parliament). Such a request must include details which allow location of the specific recorded images, including a personal description and the date, time and location of the event. It will be made clear to anyone making the request how the images will be provided, including the obscuring of any third parties identifiable on the disclosed images.

4.7 Access is limited to authorised people on a secure computer which is located in a secured office.

5 Freedom of information

5.1 As a public authority BTC may receive requests under the Freedom of Information Act 2000 (FOIA) BTC has a staff member who is responsible for responding to FOI requests, and who understands the authority's responsibilities. They must respond within 20 working days from receipt of such requests.

5.2 Section 40 of the FOIA and section 38 of the FOISA contains a two-part exemption relating to information about individuals. When any request for CCTV footage is received, consideration will be given to:

(a) Are the images those of the person making the request? If so then that information is exempt from the FOIA/FOISA, and the request will be treated as a data protection subject access request, as explained above.

(b) Are the images of other people? These can be disclosed only if disclosing the information in question does not breach the data protection principles. In practical terms, if individuals are capable of being identified from the relevant CCTV images, then it is personal information about the individual concerned. It is unlikely that this information can be disclosed in response to an FOI request as the requester could potentially use the images for any purpose and the individual concerned is unlikely to expect this. This may therefore be unfair processing in contravention of the Data Protection Act (DPA).

6 Good practice

6.1 Clear and prominent signage will be placed in the area where CCTV will be used, stating that CCTV is in operation and that the scheme is operated by BTC and giving contact details. There will be periodic checks to ensure that the signs are still in place.

7 Audits/Reviews

7.1 The following will be undertaken at least annually, and more frequently where operational reasons suggest that such review has become necessary (eg where re-siting of the camera may be deemed necessary):

(a) The use, location and direction of coverage of the camera(s) will be reviewed by BTC and TVP.

(b) The system will be periodically reviewed to ensure all legal requirements, policies and standards are complied with in practice.