Drayton Parslow Parish Council - CCTV and Surveillance Policy

1. INTRODUCTION

There is an increasing range of technologies available for the prevention and detection of crime and antisocial behaviour, many of which capture personal data on individuals. In the case of images, these are increasing in definition, and more easily able to be distributed.

Whilst these technologies provide better opportunities for the Parish Council to prevent and detect crime and antisocial behaviour in our area, we realise that this must be balanced against an individual's rights of privacy, and that unwarranted and excessive use of surveillance technologies has contributed a tougher regulatory landscape.

This policy is therefore designed to address both the powers and obligations of the Council, and the legislation protecting the rights of individuals, with particular regard to the principles of the Data Protection Act 2018, in order to ensure that the Council's use of CCTV and other surveillance technologies is lawful, safe, and reasonable.

2. LEGAL BASIS

The power for a parish council to install CCTV and other surveillance equipment is conferred under Local Government and Rating Act 1997 s.31:

(1) A parish council or community council may, for the detection or prevention of crime in their area –
(a) install and maintain any equipment,
(b) establish and maintain any scheme, or
(c) assist others to install and maintain any equipment or to establish and maintain any scheme.

The Council also has a duty to consider crime and disorder implications of their functions, under the Crime and Disorder Act 1998 s.17:

(1) …It shall be the duty of each authority to which this section applies to exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonable can to prevent,
(a) crime and disorder in its area (including anti-social and other behaviour adversely affecting the local environment); and
(b) the misuse of drugs, alcohol and other substances in its area; and
(c) re-offending in its area

Under Article 8 of the European Charter on Human Rights (enshrined in Human Rights Act 1998 Sch.1), an individual has the *qualified* right to respect for private and family life:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

However, the rights of the individual are protected with regard to the qualification under s(2) above, through the Protection of Freedoms Act 2012 s.33:
(1) A relevant authority must have regard to the surveillance camera code [created by s.29 of the Act] *when exercising any functions to which the code relates.*

The Policy Statement below further addresses the best practice set out in the surveillance camera code.

3. SCOPE

3.1 Purpose of the policy

The purpose of this policy is to enshrine within the Council's practices the *Surveillance camera code of practice*[1] and *Data protection code of practice for surveillance cameras and personal information*[2] to ensure the Council meets its statutory obligations as stated above, and to ensure that individuals and the wider community have confidence that surveillance cameras are deployed to protect and support them rather than spy on them.
[1] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
[2] https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

3.2 What is covered by the policy

This policy covers the functions currently carried out by the Parish Council:
(a) *CCTV.* The Council operates a system of 6 CCTV cameras located around Greenacre Hall and the Sports & Social Club Pavilion and both car parks at the Upper Recreation Ground, for the prevention and detection of crime and antisocial behaviour.

3.3 Who is covered by the policy

The following people and organisations are covered by this policy:
(a) *Data controller* and *data owner* – meaning Drayton Parslow Parish Council
(b) *System manager(s)* – meaning the Parish Clerk &/or the Parish Chairman
(c) *System user* – meaning such councillors, officers, or other individuals authorised to use the surveillance equipment
(d) *Data subject* – meaning any such individual whose personal information is captured by the surveillance equipment

4. POLICY STATEMENT

In accordance with the *Surveillance Camera Code of Practice 2013* the Council has adopted the following 12 principles:
1. 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.

The specified purpose of the systems listed in 3.2 is for "*the prevention and detection of crime and antisocial behaviour with the Parish of Drayton Parslow*". The systems shall not be used for any other purpose, and there shall be a prohibition on the monitoring of the lawful movements of any individual.

2. 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.

There are varying and subjective expectations of privacy, and the Council shall not:
(a) deploy surveillance camera systems in public places where there is a high expectation of privacy, including toilets and changing rooms;
(b) use any forms of audio recording in a public place, other than for the recording of Council and committee meetings
(c) use any form of facial recognition or other biometric characteristic recognition system
The Council shall also undertake a privacy impact assessment for any new form of surveillance it wishes to undertake, and shall regularly review such assessments alongside this policy.

3. 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.

The Council shall ensure that sufficient signage is in place in all areas covered by any surveillance system, and that the Council's privacy policy, CCTV and surveillance policy, complaints policy, and other relevant documents are published on its website.

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

The *Data Controller* and *Data Owner* shall have overall ownership for the surveillance systems in place, with the *System Manager(s)* having responsibility for ensuring that proper governance arrangements are in place, and ensuring that such arrangements are communicated to and adhered to by any *system users*.

5. 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.

The *System Manager(s)* will ensure that all system users are aware of the contents of this policy and have sufficient training to safely and securely use the equipment.

6. 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.

As a default, all images captured shall be deleted without review, unless the *system manager* is satisfied beforehand that there is a legitimate reason, under Principle 1, for it being accessed and viewed.
(a) *CCTV.* Images are stored on a DVR for a period of up to 30 days, following which they are automatically overwritten.

7. 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.

Access to all images by any permitted users is solely for the purposes set out in Principle 1 above. Access to stored images is restricted to the *System Managers*, and the Police where appropriate.

Where footage is extracted for the purposes of passing this to a third party (e.g. the Police or a school for the identification of an offender) the Council shall ensure this complies with any data protection legislation, and any stipulations in its Data Retention Statement and Privacy Policy. The Council shall also take reasonable steps to ensure the third party has in place practices and procedures to comply with data protection regulations. *(Data Protection Act 2018)*

Where another third party, such as a person whose property has been damaged, requests the disclosure of images, such requests will be approached with care and in accordance with the Human Rights Act 1998, and with a view to the guidance set out in para. 4.7.4-4.7.6 of the *Surveillance Camera Code of Practice 2013*.

8. 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.

The *System Manager(s)* shall ensure that all CCTV follows British Standard BS7958 on the operation and management of CCTV, and that all surveillance equipment meets the any such additional standards as made available by the Surveillance Camera Commissioner.

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

The *System Manager(s)* shall follow the guidance as outlined in *Data protection code of practice for surveillance cameras and personal information 2017.* All CCTV DVRs and SD cards used to capture images shall be password protected.

10. 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.

The *Data Controller* shall review this policy and privacy impact assessments, along with the number and positioning of all surveillance cameras, in line with the *Surveillance Camera Code of Practice 2013.*

11. 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.

The *Data Controller* shall ensure that the quality and positioning of any surveillance equipment is such so as to achieve the highest quality and most useful images, including the use of HD cameras and IR night vision. Where images are to be used for law enforcement and criminal proceedings, the Council will ensure that there is an audit trail of all images used, and that such images are available in a readily exportable format without the loss of forensic integrity.

12. ***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****.*

This may include the use of automatic number plate recognition (ANPR) or facial recognition systems. However, as stated in 2(c), the Council will not use facial and biometric recognition technology. In addition, the Council does not have, nor has no intention of using, a reference database for the purposes of matching data captured from its surveillance systems.