

Aintree Village Parish Council

Report on CCTV Policy

1.0 Purpose of report

1.1 The purpose of this report is to seek Members' approval to the CCTV Policy.

2.0 Introduction

2.1 Members will be aware that there is a CCTV camera installed and operated in the Park by Sefton Council since the 1990's. The said CCTV camera is monitored remotely by SeftonArc at its operational room in 209 Linacre Lane, Bootle, for which the Parish Council pays annual charge of some £765.

2.2 The CCTV camera is mounted on a high post situated between the Council Chamber and the Changing Room building and due its height there have been a number of complaints over the years from nearby residents believing that CCTV camera is intruding on their families' privacy when it is pointing in their direction.

2.3 Initially the CCTV camera was a major success in deterring anti-social behaviour in the Park. However over the years as it became clear that the single camera can only focus on one place at a time and consequently the anti-social behavior appears to have increased. In fact over the last couple of years there have been a number of cases of vandals climbing on the roof of the two buildings and incidents of physical bullying and intimidation. There has also been criminal damage done to the metal shutters on the window of the Park Officer's Office and the public notice board.

2.4 In response to the above the Parish Council agreed at its meeting on 15th July 2019 to the installation of some 10 additional CCTV cameras that would provide a far wider coverage of the Park, including the two buildings, and the car park, and would be managed and monitored in-house.

2.5 There are a number of Legislations covering the control and management of CCTV cameras and the purpose of this report and the attached draft policy is to ensure that the Parish Council complies fully with these regulations.

3.0 Legislations

3.1 Most CCTV schemes will be covered by the Data Protection Act, now replaced by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The Data Protection Act gives individuals the right to see information held about them, including CCTV images of them, or images which give away information about them (such as your car number plate). It also sets rules which CCTV operators must follow when they gather, store and release CCTV images of individuals. The Information Commissioner can enforce these rules.

3.2 The CCTV operator must let people know they are using CCTV. Signs are the most usual way of doing this. The signs must be clearly visible and readable, and should include the details of the organisation operating the system if not obvious.

3.3 The CCTV Operator must:-

- Make sure someone in the organisation has responsibility for the CCTV images, deciding what is recorded, how images should be used and who they should be disclosed to.

- Have clear procedures on how to use the system and when to disclose information.
- Make regular checks to ensure the procedures are followed.

3.4 Individuals have the right to see CCTV images of themselves and to ask for a copy of them. The CCTV operating organisation must provide them within 30 calendar days. This is called a Subject Access Request. Individuals will need to provide details to help the operator to establish their identity as the person in the pictures, and to help them find the images on their system.

3.5 CCTV operators are not allowed to disclose images of identifiable people to the media - or to put them on the internet - for entertainment. Images released to the media to help identify a person are usually disclosed by the police.

3.6 The CCTV operating organisation may need to disclose CCTV images for legal reasons - for example, crime detection. Once they have given the images to another organisation, then that organisation must adhere to the Data Protection Act in their handling of the images.

3.7 Public authorities are subject to the Freedom of Information Act 2000. This Act allows members of the public to request official information by writing to the public authority, who must respond within 20 working days. If the images are those of the person making the request, then the request would be handled under the Data Protection Act as a Subject Access Request. If, however, other people are identifiable in the CCTV pictures, then the images would be considered personal information and it is likely they would be exempt from the Freedom of Information Act.

3.8 CCTV operating organisations should have a retention policy. They should only keep the images for as long as necessary to meet the purpose of recording them.

4.0 Legal Implications

4.1 The Parish Council must comply with all the relevant legislations, including the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and Freedom of Information Act 2000.

5.0 Financial Implications

5.1 Subject to complying with the relevant legislation there are no financial implications as a result of this report.

5.0 Recommendation

5.1 It is recommended that Members note the content of this report and approve the CCTV Policy attached as Annex A to this report.



AINTREE VILLAGE PARISH COUNCIL

CCTV Policy

20th January 2020
Minutes XXXX

AINTREE VILLAGE PARISH COUNCIL

CCTV Policy

1.0 Introduction

- 1.1 The aim of this policy is to control the management, operation, use and confidentiality of the CCTV system located in Council Chamber, Harrow Drive, Aintree Village. The site is owned and managed by Aintree Village Parish Council.
- 1.2 The policy was prepared after taking due account of the Code of Practice published by the Data Protection Commissioner (revised 2015) and the General Data Protection Regulations 2018. This policy will be subject to periodic review by the Parish Council to ensure that it continues to reflect the public interest and that it and the system meets all legislative requirements.
- 1.3 The CCTV Scheme is registered with the Information Commissioner under the Terms of the Data Protection Act 1998. Registration Reference: **ZA249520**.
- 1.4 Aintree Village Parish Council accepts the eight data protection principles based on the Data Protection Act 1998 as follows. Data must be:
- a) fairly and lawfully processed;
 - b) processed for limited purposes and not in any manner incompatible with those purposes;
 - c) adequate, relevant and not excessive;
 - d) accurate;
 - e) not kept for longer than is necessary;
 - f) processed in accordance with individuals' rights;
 - g) secure;
 - h) not transferred to a country or territory outside the European Economic Area unless an adequate level of protection for the rights and freedoms of data subjects is ensured.

2.0 Statement of Purpose

- 2.1 To provide a safe and secure environment for the benefit of those who might visit, play, work in the Park. The system will not be used to invade the privacy of any individual, except when carried out in accordance with the law. The scheme will be used for the following purposes:
- to reduce the fear of crime by persons using facilities in the Park, so they can enter and leave the buildings and facilities without fear of intimidation by individuals or groups;
 - to reduce the vandalism of property and to prevent, deter and detect crime and disorder;
 - to assist the police, the Parish Council and other Law Enforcement Agencies with identification, detection, apprehension and prosecution of offenders by examining and using retrievable evidence relating to crime, public order or contravention of bye-laws;
 - to deter potential offenders by publicly displaying the existence of CCTV, having cameras clearly sited that are not hidden and signs on display in areas being

- monitored;
- to assist all “emergency services” to carry out their lawful duties.

3.0 Changes to the Purpose or Policy

3.1 The CCTV Policy may be discussed at meetings of the Park and Amenities Committee. However, any major change that would have a significant impact on either the purpose or this policy of operation of the CCTV scheme will take place only after discussion and resolution at a full Parish Council meeting.

4.0 Responsibilities of the Owner of the Scheme

4.1 Aintree Village Parish Council retains overall responsibility for the scheme.

CCTV Code of Practice

1.0 Management of the System

- Day to day operational responsibility rests with the Council Manager and Parish Clerk to the Council and Chair of the Park and Amenities Committee. Breaches of this policy will be investigated by the Council Manager and Parish Clerk to the Council and reported to the Parish Council. A CCTV system prevents crime largely by increasing the risk of detection and prosecution of an offender.
- Any relevant tape or digital evidence must be in an acceptable format for use at Court hearings. This policy must be read and understood by all persons involved in this scheme and individual copies of this policy will therefore be issued for retention. A copy will also be available for reference in the secure recording areas.

2.0 Control and Operation of the Cameras, Monitors and Systems

The following points must be understood and strictly observed by operators:

- a) Trained operators, which will include the Park Officer and the Assistant Park Officer must act with integrity and not abuse the equipment or change the pre-set criteria to compromise the privacy of an individual.
- b) The position of cameras and monitors have been agreed with SeftonArc, which is owned by Sefton Council.
- c) No public access will be allowed to the monitors except for lawful, proper and sufficient reason, with prior approval of the Council Manager and Parish Clerk to the Council or the Parish Council. The Police are permitted access to tapes and prints if they have reason to believe that such access is necessary to investigate, detect or prevent crime. The Police are able to visit the Park to review and confirm the Parish Council’s operation of CCTV by arrangement. Any visit by the Police to view images will be logged by the operator.
- d) Operators should regularly check the accuracy of the date/time displayed.
- e) Storage and Retention of Images - Digital records should be securely stored to comply with data protection and should only be handled by the essentially minimum number of persons. Digital images will be erased after a period of 31 days.

- f) Images will not normally be supplied to the media, except on the advice of the police if it is deemed to be in the public interest. The Council Manager and Parish Clerk would inform the Chairman of the Parish Council of any such emergency.
- g) As records may be required as evidence at Court, each person handling a digital record may be required to make a statement to a police officer and sign an exhibit label. Any images that are handed to a police officer should be signed for by the police officer and information logged to identify the recording, and showing the officer's name and police station. The log should also show when such information is returned to the Parish Council by the police and the outcome of its use.
- h) Any event that requires checking of recorded data should be clearly detailed in the log book of incidents, including Crime Numbers if appropriate, and the Parish Council notified at the next available opportunity.
- i) Any damage to equipment or malfunction discovered by an operator should be reported immediately to the Council Manager and Parish Clerk then to and then to the Parish Council and recorded in the log. When a repair has been made, this should also be logged showing the date and time of completion.
- j) Subject Access Requests - Any request by an individual member of the public for access to their own recorded image must be made on an Access Request Form. Forms are available by contacting the Council Manager and Parish Clerk to the Council or can be downloaded from the Parish Council website and will be submitted to the next meeting of the Parish Council for consideration and reply, normally within one calendar month. There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee

3. Accountability

Copies of the CCTV Policy are available in accordance with the Freedom of Information Act, as will any reports that are submitted to the Parish Council providing it does not breach security needs. The Police will be informed of the installation and provided with a copy of this CCTV Policy. Any written concerns or complaints regarding the use of the system will be considered by the Parish Council, in line with the existing complaints policy.

THIS POLICY MUST BE COMPLIED WITH AT ALL TIMES.

Access Log Book

Date/time	Who had access?	Why access granted/required?	Result of access – viewing details	Any other comments
<i>e.g. 1st February 2020 at 10.30am</i>	<i>Frank Boyle</i>	<i>Complaint received regarding verbal abuse near the Tuck Shop</i>	<i>Data viewed-confirmed incident – perpetrator could be identified from images – reported to the police</i>	<i>Informed the Council Manager and Parish Clerk</i>