Policies & Procedures Relating to The Use of Staple Parish Council's CCTV Camera:

This Document:

- An overview of additional assessments made during the preparation of this document can be found in Appendix 1
- A list of the abbreviations used in this document can be found in Appendix 2, section 1.
- This document has been produced following extensive use of information, guidelines, recommendations and legal requirements referred to in material from The Information Commissioner's Office (ICO.org.uk). A more detailed list of publications / agencies contacted or referred to can be found in Appendix 2, section 2.
- Requests that this document be reviewed/amended/updated/improved can be made at any time. (Such requests should be made to Staple Parish Council.)
- This document will be reviewed annually.

Background:

- Following reports of drug dealing in Staple, specifically in the driveway of the Village Hall; the Parish Council discussed the possibility of installing a CCTV camera as a deterrent/means of recording the crimes.
- The Parish Council subsequently deemed the installation of a CCTV to be a proportionate response to the problem.

Location and Scope:

- The Camera is fixed to the underside of a soffit on the end elevation of the Village Hall, adjacent to the driveway.
  (It is mounted out of reach, and its power lead is encased within a cable protection cover.)
- The camera's area of view covers only the village Hall's driveway. (**It does not cover any other areas; such as those used by Pre-school; or the public highway**).
- The camera is an IP device, and its stored footage is only accessible wirelessly.
  The wireless signal carrying this footage is encrypted; thus making interception impossible.
- As a privacy-protection measure, audio recording has been disabled. **(And will not be re-enabled**).
- There is a prominently displayed sign on the end wall of the Village Hall informing those in the vicinity that CCTV is in operation. Staple Parish Council will ensure that this sign is always well-maintained /clearly visible.
- **The CCTV camera will only be used for the purpose for which it was purchased**. i.e. to deter/record incidences of drug-dealing or other illegal activities in the driveway of the Village Hall.

Use, Responsibilities and Access:

- The CCTV camera is the responsibility of Staple Parish Council.
  It is owned, managed and maintained by Staple Parish Council.
  Thus, in accordance with ICO's/GDPR's codes of practice, Staple Parish Council are deemed to be this system's 'Data Controller'. (n.b. In this context, 'data' refers only to the CCTV's stored footage).
- The CCTV footage will only be accessed from a dedicated device. i.e. a password-protected laptop reserved for that purpose. (**And won't in any circumstance be accessed from a personal device**.)
  The laptop will contain no other programmes; and will not have access to any "cloud" storage systems.

Use, Responsibilities and Access (contd.):

- A log of any access to the stored data will be kept.
- Any queries regarding the CCTV camera or the Policies and Procedures relating to the camera should be directed to the Parish Council.
- Similarly, any requests for access to the CCTV footage should be directed to the Parish Council.
- A record of all access requests will be made and kept. This record will include the name of the person making the request/ the organisation they represent/ the reason they require access / how the request was dealt with.
- Disclosure of information from Staple Parish Council's CCTV camera will be controlled; and will be consistent with the purpose for which the system was established.
- Disclosure of the information referred to above will only be permitted in two very specific circumstances: i.e. Subject access requests; and requests from Law Enforcement Agencies. (**No other access requests will be considered**).
- Staple Parish Council will comply with any updates to the relevant ICO/GDPR requirements relating to the use of its CCTV; and will update this document to reflect this.
- In line with recommended codes of practice from the ICO / following GDPR recommendations, Staple Parish Council decided (following unanimous approval of a proposal at its the Staple Parish Council Meeting of November 10th; Agenda item 8.1.1) that **the number of people able to access the CCTV's stored data would be limited to a single, DBS-checked individual: David Kirk.**
- CCTV footage will be stored for the minimum period necessary, after which it will be deleted. This period is currently 31 days; but this can be amended following discussion/decisions made by Staple Parish Council (SPC); either SPC-initiated, or following requests from external sources.
- Irrespective of whether or not the stored footage has been accessed; it will automatically be overwritten once the device's storage limit is reached.
- Copies of this document will be made available upon request; and will be published on the Parish Council's web site.
- Access to the stored footage is only possible upon the successful entry into the receiving device of an end-to-end encrypted username and password.
  (The initial username/password used to install and test the system have since been replaced by the sole user.)
- The identity of those recorded on the CCTV camera's footage isn't sought/required/noted/disclosed.
- The CCTV footage is simply stored and then deleted. (It is isn't further 'processed').

Subject Access Requests:

- All subject access requests for CCTV footage are subject to the following conditions:

  i) A subject access request will only be considered where the applicant can show reasonable cause to believe that Staple Parish Council currently possesses CCTV footage in which the applicant personally can be seen and accurately identified.
  ii) A subject access request will only be considered alongside the privacy rights of any other individuals whose image may appear in the same footage.
  iii) A subject access request may be denied if Staple Parish Council has concerns about the risk of prejudice or harm to other individuals through their identification.
  iv) People making subject access requests for CCTV footage will be required to supply a personal photo identification document (e.g. passport or photo-card driving licence.)

APPENDIX 1. Data Protection Impact Assessment (DPIA:)

ICO Guidelines on DPIA's:

ICO guidelines state that in certain circumstances, prior to installing a CCTV:

- A DPIA should be carried out.
- Carrying out a DPIA isn't mandatory for every processing operation; and is only required when the processing is likely to result in a "high risk to a person's rights and freedoms".
- It is up to each organisation to decide whether its processing is of a type likely to result in a "high risk"; taking into account the nature, scope, context and purposes of the processing.

Requirement for DPIA's:

- GDPR doesn't define what constitutes a 'high risk to a person's rights and freedoms'.
- A catalogue of ten criteria (article 29 of the GDPR Working Party) indicates when processing may bear a 'high risk' to a person's rights and freedoms.
- The ICO's guidance states that a DPIA is not necessary if a processing operation only fulfils one of the ten aforementioned criteria.
- The ICO's guidance states that if "several criteria are met, the risk for the data subjects is likely to be high; and a DPIA is thus required".

GDPR's criteria for determining what categories of data processing constitute 'high risk' :

1) Scoring/profiling
2) Automatic decisions which lead to legal consequences for those impacted.
3) Regular and systemic large-scale monitoring of data subjects.
4) Processing of special personal data.
   (incl. data that reveals a subject's political opinions, religious beliefs, trade union membership, criminal convictions)
5) Large scale data processing.
   (e.g. processing that brings together technologies such as Distributed Systems, Machine Learning, Statistics, and Internet).
6) The merging or combining of data which was gathered by various processes.
7) Data about incapacitated persons or those with limited ability to act.
8) Use of newer technologies or biometric procedures.
9) Data transfer to countries outside the EU.
10) Data processing which hinders those involved in exercising their rights.

- DPIAs are primarily concerned with the processing of data; rather than the recording of CCTV footage.
- DPIAs are particularly useful when CCTV operations are combined with drone surveillance, body-worn cameras, facial recognition technology, automatic number plate recognition (ANPR) and audio recording.
- With reference to the above information; and given that the use of Staple Parish Council's CCTV operations match none of the ten criteria mentioned above; the carrying out of an intensive, formal DPIA was deemed to be unnecessary.
- Section 9 of the ICO's guidelines on DPIAs recommends that where a new surveillance camera system is introduced you must "*consider* a DPIA". In lieu of an intensive, formal DPIA; a basic assessment of the impact on the safety, privacy/anonymity/freedoms and rights of those likely to be recorded by the system was made. And this resulted in the conclusion that the installation of the CCTV system was a justified and appropriate measure which wholly met, but didn't exceed, the specific requirements/purpose for which it was purchased.

APPENDIX 2.

2.1 Abbreviations used in this document:

CCTV Closed Circuit Television
GDPR General Data Protection Regulation
OFSTED The Office for Standards in Education, Children's Services and Skills
DPIA Data protection Impact Assessment
VHC Village Hall Committee
ICO Information Commissioner's Office
SPC Staple Parish Council

2.2 Documents, Codes of Practice, Legislation, Organisations Referenced / Contacted (To assist in the formulation of Staple Parish Council's CCTV camera's Policies & Procedures Document):

Conversations with organisations:

- **OFSTED**
  (n.b. OFSTED confirmed that due to the field of view of SPC's CCTV camera, they had no issues with it).

- **Information Commissioner's Office.**
  (n.b. The ICO provided valuable advice; particularly in relation to DPIAs).

- Staple Pre-School Trustees. (Via their VHC rep.)

- Staple Village Hall & Recreation Management Committee.

Publications / Codes of Practice, Legislation Referenced:

- Data protection impact assessments: Guidance for carrying out a data protection impact assessment on surveillance camera systems.
  (A publication jointly produced by The Surveillance Camera Commissioner and the ICO)

- CCTV Guidance: Information for setting up and using CCTV cameras.
  (Home Office April 2009, Updated 2016)

- Surveillance Camera Code of Practice June 2013 (Home Office)

- Surveillance camera code of practice: Consultation on revision to the 2013 Code.
  (Home Office September 2021)

- Surveillance camera code of practice: case studies
  (Home Office July 2015, Updated October2021)

- *In the picture*: A data protection code of practice for surveillance cameras and personal information (ISO).

- The Protection of Freedoms Act 2012. (The regulation of public space surveillance cameras).

- The Regulation of Investigatory Powers Act (RIPA) 2000

- Surveillance Camera Code of Practice: A Guide for Councillors (Surveillance Camera Commissioner).