INGOL AND TANTERTON NEIGHBOURHOOD COUNCIL CCTV Policy

Ingol and Tanterton Neighbourhood Council (NC) is a local council made up entirely of elected or co-opted members and an employed Clerk who manages the business of the council. The NC is host to a few CCTV systems. The NC has adopted the Home Office 'Surveillance Camera Code of Practice' issued in June 2013 and has therefore agreed to abide by the following 12 'Guiding Principles' from the Code of Practice:

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 legitimate aim is to protect the areas of the neighbourhood and particularly its residents from Anti-Social Behaviour (ASB), Vandalism, Criminal Damage, the Threat of Violence and any other potential problem that residents may encounter.

2. The use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

Regular annual reviews of the Privacy Impact Assessment will be undertaken to ensure that the CCTV system remains justified in its use.

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.

Signage informing residents is prominently placed in the area under surveillance. The contact person is the Clerk to the Council. He can be accessed through ingoltantertonnc@hotmail.co.uk or by telephoning 01772733829.

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

The only person authorised to operate the CCTV system is the Clerk to the Council. He is the responsible person. No images are to be stored on any computer other than those computers which are linked into the systems.

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.

Signage is in prominent positions near the areas of surveillance. A copy of the Council's CCTV policy is placed on its web site

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.

The CCTV hard drive is an automatic overwrite system with approximately 30 days storage capacity.

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 the CCTV recording system's hard drive is by the Clerk who is the data controller and will only be accessed when an event occurs that requires investigation and that will only be done by specific request stating the range of times in which the event might have occurred and such information derived will then only be released to the police as part of an investigation or to an Authority which has the power of enforcement.

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 NC follows the Home Office Surveillance Camera Code of Practice. The Clerk will with the aid of the certified CCTV installation company be kept up to date with any training or standards relevant to the operation of the CCTV system and the NC will ensure that adequate training is provided to the Clerk as required.

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

The CCTV systems are password protected and the password restricted to the Data Controller. Where equipment is located on third party sites the hard drive is protected by a locked metal box which can only be opened by the Data Controller to allow a monitor to be connected as required for viewing by the Data Controller only. Access to the images on the hard drive can be done remotely through the Clerk's computer which is password protected. The viewing software is also 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 Clerk as the sole employee and Data Controller will be responsible for ensuring legal requirements, policies and standards are complied with.

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.

All issues arising from the stated aims for the CCTV system WILL be reported to the Police or other enforcement authority.

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.

No images will be stored by the NC beyond the hard drive capacity(approx 30 days) and no cross referencing to any data base will be undertaken by the NC