Longwick-Cum-Ilmer
Parish Council

PRIVACY IMPACT ASSESSMENT

FOR LONGWICK PLAYING FIELD

CCTV SYSTEM

Contents

1. Need for a Privacy Impact Assessment

The project under assessment is a scheme at Longwick Playing Fields in Longwick, the System being sited at Longwick Playing Fields is for the purpose of prevention and detection of crime (the "Scheme").

The project introduces the further aspect of a separate person (the "Area Coordinator") being granted remote access to the cameras at Longwick Playing Fields to allow interrogation of the CCTV System in response to a crime. In this context the term Area Coordinator may either be a nominated lead individual and a number of nominated deputies; or it may be an appropriately chosen company who may charge for acting in this role, for example a professional CCTV Security Company.

The overall Scheme shall have an owner (the "Scheme Operator") which may be a Parish Council, Residents' Association, Neighbourhood Watch area or similar body.

The use of CCTV Systems is already well established and the rules surrounding such systems are well-documented on the ICO website, however the need for a PIA results from the additional element of remote access to systems by a defined set of third party individuals. This document seeks to assess the impact of that additional element, whilst at the same time reasserting the general principles that will be followed for the Scheme as a whole.

2. Information Flows

The information flow under assessment will be that of the recorded footage held on a standard CCTV System Digital or Network Video Recorder ("DVR" or "NVR") sited at one or more areas within the area covered by the Scheme. In all cases the owner will act as the Data Controller for their CCTV System and shall have the discretion to allow access to, and downloads from, their CCTV System.

The CCTV cameras record continuous footage onto an internal hard drive within the DVR/NVR. Recorded footage will usually contain 'personal' information as defined by the Data Protection Act (the "DPA"), such as images of people, and images of vehicles which may include registration numbers where cameras are of sufficient quality or are designed specifically to read registration plates, i.e. an ANPR Camera.

Initial information flow regarding details of crimes will come from both the Police and from local residents using standard communication methods already in use, for example email. This information will be shared directly with all residents in the Scheme but specifically to the Area Coordinator.

The Area Coordinator will have the ability to search specific cameras on the CCTV Systems referred to. If evidence is found on a CCTV System, one of two scenarios will follow:

a) The Area Coordinator will download the footage as evidence to local storage on their personal computer from where it will be written onto optical media, (CD or DVD) or a USB Stick, or sent via which ever method the Police dictate, or handed it to the Police with an Evidence Statement under standard protocols if using a CD/DVD/USB. Under this method the Area Coordinator acts as a Data Processor for the data.
b) The Area Coordinator will alert the Police directly, with the address of the property where the DVR/NVR is located, along with the relevant date, time and camera positions. The Police will then attend the property to download that footage directly, in line with their own existing protocols. If a digital version can't be obtained.

To end the information flow the data recorded on the DVR/NVR will be destroyed by virtue of being automatically overwritten after a reasonable time; any footage downloaded to the Area Coordinator's PC must also be destroyed after a suitable period of time; and any footage passed to the Police will fall under their existing protocols for the handling of such data.

Privacy risks arise within the Scheme in two categories: firstly the siting of the CCTV cameras; and secondly the use and control of any downloaded footage. This document will assess these two areas in section 3.

3. Privacy and related risks

In this section, privacy risks are examined by reference to the eight Data Protection Principles. Each risk listed is then addressed in Section 4 of this document.

3.1. Principle 1: Fair and lawful

Personal data shall be processed fairly and lawfully. In particular, it shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The purpose of the Scheme is to aid the prevention and detection of crime, and therefore has a legitimate purpose.

CCTV footage will not be used in ways that have unjustified adverse effects on the individuals concerned. The Scheme does not interfere with an individual's right to

privacy because footage will only be searched and downloaded in relation to actual crimes that have taken place at a given location.

The social need and aims of the Scheme are to assist the Police in the detection of crime. The Scheme is a proportionate response to the problem of crime because criminals are becoming increasingly forensically aware, and it has been proven in many cases that CCTV footage from residents has been the only evidence that has allowed the Police to identify and subsequently arrest the perpetrators.

Evidence from such a Scheme has previously been tested at Crown Court without challenge, resulting in successful prosecution in relation to an aggravated burglary.

3.2. Principle 2: Purposes

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Footage will be downloaded for the single lawful purpose of providing evidence in relation to a specific crime that has taken place at a given location.

3.3. Principle 3: Adequacy

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

The CCTV Systems deployed by residents as part of the Scheme will vary in image quality. Any image of activity at or near the scene of a crime can be relevant and helpful in solving the crime, even if the individuals or vehicles cannot be identified, for example an image of a person entering and taking a car in the distance may pinpoint the time that the event took place. This can be combined with other known facts by the Police as part of the overall investigation.

Personal data downloaded as part of the Scheme will include facial imagery and vehicle registration marks (VRMs) where cameras are of sufficient resolution to capture these. Both of these elements of data are relevant and essential for the stated purpose of helping the Police to solving crime.

As domestic CCTV Systems are now readily available which have ANPR capability, it must be understood that these systems do not provide any additional information than could otherwise be obtained by viewing the footage by eye and writing down the VRM of each passing vehicle. Capturing of VRMs on CCTV footage is permitted provided that the CCTV System is not directly linked to a database that identifies any other information about the owner of that vehicle. This identification activity is the

sole responsibility of the Police. CCTV Systems registered with the Scheme will not be linked to any such database relating to ownership.

CCTV owners who register under the Scheme will supply their name, address and DVR/NVR login details to the Area Coodinator who will only make these details available to nominated deputies.

3.4. Principle 4: Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

Members' details will be retained by the Area Coordinator and updated as necessary. Failure to keep up to date information will result in failed attempts to solve crimes. Members also have an onus to advise the Scheme with which they have registered of any change of details.

Accuracy of CCTV imagery relies on the timestamp of any footage downloaded, and the Area Coordinator must ensure that the time offset of any footage downloaded is recorded against an accurate time source. This will avoid the possibility of the wrong data subject being identified for a specific crime due to such an inaccuracy.

The time stamp on most modern DVRs/NVRs is regulated by an automated process. They link to either time servers e.g. time.windows.com or in the case of Hikvision DVRs/NVRs they can link to the Hik-Connect cloud service and keep the time accuracy to within a second, auto updating daylight saving time.

3.5. Principle 5: Retention

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

CCTV Systems generally operate by default in overwrite mode. This means that once the internal hard drive is full the DVR/NVR will record new footage by overwriting the oldest footage currently stored on the hard drive. The length of time that footage is preserved before being overwritten is determined by the recording settings and the amount of space available on the hard drive. Typical systems retain footage for about 4 weeks before being overwritten, however a maximum retention time of 8 weeks is recommended for use within the Scheme. This period is calculated to allow for delays in obtaining information about a crime, and then allowing sufficient time for the Scheme operator to search and download from each system which may have recorded evidence of the reported event.

In cases where the Area Coordinator downloads footage that is presented as evidence to the Police, they should agree with the Police who will retain the Master of the

footage. It is acceptable for the Area Coordinator to retain the Master under such an agreement, and a suitable retention period would be 7 years. The storage of such evidence is covered under section 3.7.

Where footage does not eventually become evidence, that data should be deleted after a suitable period as documented by the Scheme. In summary, the Scheme must decide and document retention periods for each type of data and ensure that those are adhered to.

3.6. Principle 6: Rights

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Email alerts regarding crimes will be sent to CCTV owners who have registered with the Scheme, and those emails will carry instructions for how individuals can opt out of receiving those emails.

Any Subject Access Requests ("SAR") will be made directly to the CCTV System owners as Data Controllers, and the introduction of an Area Coordinator as a Data processor does not change this. The Area Coordinator may assist in the execution of an SAR presented to a CCTV System owner.

3.7. Principle 7: Security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

CCTV Systems must be registered under the DPA. Instructions must therefore be given to CCTV owners who register under the Scheme as to how to operate their CCTV system securely to remain compliant with the DPA.

In any situation where the Area Coordinator or a deputy changes, System passwords must be changed so that access to the CCTV Systems is denied.

Consideration must be given to the choice of Area Coordinator and any deputies, and how approval by the CCTV System owners of the individual(s) selected should be sought. In order to preserve privacy, remote access should only be granted to the Area Coordinator for front-facing cameras at a property/location, not having access to any cameras that can look into someone's property where implied access is not granted. For instance, someone's back garden. The exception is where the Area Coordinator is a company whose role may also include, for example, the general setup and maintenance of the CCTV System.

Footage stored on the DVR must have appropriate access controls applied. The only individuals who should be able to access the data should be the CCTV System owner, the Area Coordinator, and the CCTV installer for the purposes of service and maintenance or to download footage at the owners request. All of these are reasonable in the context of security.

Footage must only be downloaded by the Area Coordinator with express permission and knowledge of the Data Controller for the CCTV System, and any footage downloaded by the Area Coordinator must be stored securely. For example the PC onto which it is downloaded should, as a minimum, be password protected using a strong password and have a suitable firewall installed. Hard drive encryption should be considered.

Evidence Masters retained by the Area Coordinator must also be stored securely and a register retained of each item held, passed on or destroyed. Storage in a lockable safe should be considered, at least to demonstrate whether such data has been compromised.

3.8. Principle 8: International

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

There are no international aspects to the Scheme.

4. Privacy Solutions

The wording of Section 3 of this document already addresses the methods of operation of such a Scheme to ensure compliance with the DPA. If a Scheme operator foresees any other risks these should be documented along with the mitigation plan, and stored safely for inspection by the ICO.

5. Signoff

The Scheme Operator shall print and sign a copy of this document to show that all of the statements in Sections 3 have been understood and will be complied with.

Any specific solutions implemented to implement risks should be recorded and attached to that signed copy at the time of signature.

6. Implementation

The Scheme Operator is responsible for implementing the solutions that have been approved and for assigning a contact person for any privacy concerns which may rise in the future. Those who take part in the Scheme should be notified of the method of contacting that person as part of the registration process

Any actions that have yet to be undertaken at the time of approving the Scheme should be recorded and attached to the signed copy of this document at the time of signature, along with appropriate dates for completion and review.

Implementation sign off

Scheme Operator (e.g. XYZ Residents Assoc.)	Longwick-Cum-Ilmer Parish Council
Area Co-ordinator (name of person or company)	Valeri McPherson - Chairman
Deputy 1 (if none put "N/A")	Richard Myers – Vice Chairman
Deputy 2 (if none put "N/A")	Tracey Martin - Clerk
Deputy 3 (if none put "N/A")	Mark Molson – Councillor
Designated Security Company for service an maintenance	Camsec Security Ltd: Phil Jarvis – Director Chris Troughton - Director
Additional risks, notes, mitigation strategies and closure dates (if none put "N/A")	Only the above persons will have access to the system. The NVR on site is locked inside a metal security cabinet which is located inside a locked garage. The system has a 4G internet link, with no hard wired internet option onsite. The keys for the garage and CCTV cabinets are held by the Parish council. A physical plate is located behind the main PTZ camera preventing being able to see in the house holds behind the field. The ANPR camera covers only the entrance/exit roadway. The PTZ camera is programmed to only look within the confines of the field, and has digital limits to prevent it from looking into the houses next to the field. The Parish Council members listed above will be trained on how to use the system in accordance with compliance to the law. They will hold their own policy on subject access requests, and communication methods with the police.
Signatures