# Privacy Impact Assessment

## Use of drones for overt policing purposes

**Introduction:**

This document has been written in consultation with the Information Commissioner's Office and should be read in conjunction with the Information Commissioner's Conducting Privacy Impact Assessments code of practice

The template below is designed to give those Forces operating, or thinking of using drones in overt operations, a structure for completing a PIA. (Privacy Impact Assessment) It is recommended that a PIA is conducted at an early stage in project planning. The template and examples within are intended as illustrations and are not a definitive document. Individual Forces may use their own template if they so wish.

The Information Commissioner describes a PIA as 'a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.' As well as a tool for managing risk, this template can also be used to present the justification for the use of drones. This should be proportionate, legitimate and necessary. Evidence to support the effectiveness of drone use is helpful. The development of a PIA need not be a time consuming or arduous process and very much follows the lines of risk registers we are familiar with using within the Police Service. The process encourages engagement with people within our own organisation in addition to partners and local communities to identify and reduce privacy risks. By identifying these at an early stage, putting processes in place to address privacy risk should be simpler and more cost effective. Conducting a PIA should be beneficial by producing a better project plan or Force Policy, building public confidence in how the Police Service uses drones and reassuring them that drones will be used only when appropriate and necessary.

The public has concerns that drones intrude on Privacy. These concerns are heightened when the use of drones by the Police is discussed. Particular concerns associated with drones are that they are capable of operating in vantage points where individuals would have a reasonable expectation of privacy. Additionally, there are challenges associated with informing individuals about a drone being used. The capabilities and activities of both the drone and the camera should be considered as well as the wider system in which they operate.

A PIA can be used to reassure the public that police forces are using drones in a transparent way that reduces privacy intrusion. Ideally, the PIA will be started at an early stage so that identified privacy risk can be reduced through purchasing decisions. The PIA should then be updated as implementation progresses and consideration should be given to reviewing it every 12 months, or when there are changes to operations using drones. It is advisable for police force drone project leads to work together with force data protection practitioners when conducting the PIA.

# Sussex and Surrey Police Drone PIA

**Step 1 –Aims**

The data controllers for all personal data held by Sussex and Surrey Police are the respective Chief Constables. (Not including data held by the Offices of the Police and Crime Commissioners, respective Police Federations and Unison.)

Use of Drones by the Police Service is still in in its infancy. Our aims in using drones are:

- Prevention and detection of crime
- Apprehension and prosecution of offenders
- Enhance the safety of the Public and our Officers and Staff.
- Realise operational efficiencies

The purposes for processing the personal data that will be obtained are outlined below?

- Prevention and detection of crime
- Apprehension and prosecution of offenders
- Maintenance of law and order
- Protection of property
- Public Safety
- Rendering assistance to members of the public.

Drones are used to:

- Provide situational awareness to Officers and Commanders in a variety of Policing situations
- Assist with searches for Missing Persons
- Assist with investigations into Road Traffic Crashes, Major Crime and Industrial Accident investigation
- Assist with Event Planning and Management.

Surrey and Sussex Police drones are only deployed for specific operational tasks and are not used for general patrol/surveillance. I.e. they are not routinely patrolling the skies above Surrey and Sussex.

**Benefits**

Drones assist Surrey and Sussex Police to deliver a more effective Policing Service by:

- Enabling best use of resource, resolving incidents more quickly thereby providing efficiencies.
- Allowing commanders to deploy the right resources to the right location enabling Force resources to be used more effectively.
- Enhance the safety of Public and Police by deploying a drone into situations which would otherwise involve risk to individuals
- Provide good quality evidence to assist apprehension and prosecution of offenders.
- Enhance interoperability between blue light services by being used to achieve other service objectives such as Search and Rescue, Fire scene management, Casualty location and triage.

**Why has the need for a PIA been identified?**

Drones are a new technology that has the capability to capture personal data. They are perceived as being Privacy intrusive and they have the potential to drive action against individuals that can have a significant impact on them. E.g. Evidence gathering and prosecutions resulting in conviction and possible loss of liberty.

**Step 2 – Information flow and data security**

Images and video are collected by the drone being operated for policing purposes. They are stored on an SD card either within the drone itself, or transmitted via an encrypted feed to the ground station controller and recorded on an SD card within the controller. The information from the card is then downloaded into a standalone computer system located in a secure police station. Access to the system is password protected. Each person granted access creates their own unique password. Data is examined and images and video pertinent to deployment or required for evidential purposes is retained. All other images and video are deleted after 28 days.

The number of individuals that may be affected by drone operations can be difficult to determine. This is dependent on the nature of deployment, time, geography, weather. If operated in public areas it is not known how many persons will be there. These factors can have an impact on privacy risk. The PIA enables data controllers to unpick compliance risks.

**Raising Awareness and Transparent Use**

Prior to the implementation at the first trial site key landowners were contacted and permission sought to operate the system over their land. All local contacts were then briefed by email and opportunity given to respond with concerns. A show and tell day was organised and 400 plus people invited. No one attended and no one refused permission to operate.

Press releases went out in local and national newspapers in addition to social media. Local TV stations carried the story and the Police and Crime Commissioner debated with Big Brother Watch on breakfast TV. Big Brother watch were invited to visit and see the system in operation. They did not take up the invitation.

Expansion of the trial was publicised via local and national media in addition to social media. Local Neighbourhood teams engaged with their local communities. Information on the drones was placed on the external website.

A twitter account has been set up specifically for our drone use. Sussex Eye outlines where and how the drones are being used in line with the Force social media policy. We have not had any adverse reactions on this account or on any other social media.

Drones have also been used to engage with the public by providing aerial imagery for the Force contribution to Sussex day on Social Media.

**Step 3 – Risk Register**

Outline the privacy risks and the actions taken to mitigate them.

(Examples of risks and control measures are provided for guidance only and not definitive.)

| Privacy Risk | Owner | Solution/Control Measure | Result: Is the risk eliminated, reduced or accepted? | Evaluation: is the final impact on individuals, proportionate justified and compliant? | Outcomes integrated into Project Plan/Force Policy.<br><br>Action/Date | Approved by: |
|---|---|---|---|---|---|---|
| The capability of the camera may be obtaining more personal data than is needed to fulfil the purpose. E.g. through zoom and or/third party data capture | Project Lead | Training of drone operators to include guidance on prevention or inadvertent video or image capture.<br><br>Camera viewing direction adjusted. | Reduced | Yes | Training in respect of Data Protection Act, covering storage and handling and surveillance camera commissioners Codes of Practice has been incorporated Into operators training<br><br>Completed | |
| Drones are flying and recording in spaces where individuals' expectations of privacy are high. E.g. schools, back gardens, beaches, windows | Project Lead | Drones only deploy to specific incidents<br><br>Should the need arise to fly over back gardens Where practicable permission gained from householder/landowner prior to flight.<br><br>Flights over buildings and occupied beaches/land only conducted in an emergency unless occupiers of the space informed and give the | Accepted | Yes | Deployment process outlined in Operations manual. All operators have received appropriate training.<br><br>Completed | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | opportunity to move | | | | |
| Individuals filmed by the cameras may not be aware that they are being recorded. | Project Lead | Operators clearly identified as operating a drone, by signage and High Visibility Clothing.<br><br>Where practicable permission gained from householder/landowner prior to flight.<br><br>Where practicable drone flights publicised on website/social media. | Accepted | Yes | Ensure A board signs are available to operators deploying system<br><br>By December 2016<br><br>Operators instructed to wear standard Police High Viz clothing.<br><br>Completed | |
| Data is at risk if the drone is lost | Project Lead | Visual Line of sight operations only.<br><br>Drone has auto return safeguard if signal is lost or problem detected<br><br>Operators undergo CAA accredited training<br><br>Proven reliability of system.<br><br>Knowledge of system required to extract SD card | Accepted | Yes | All operators trained to CAA standard. Operations manual outlines parameter of operation is Visual Line of Sight<br><br>Drones purchased have return to home safeguard.<br><br>Completed | |
| Data is at risk when it is being transmitted | Project Lead | Data transmitted by the drone is encrypted. To Govt standard | Accepted | Yes | Drones purchased have encrypted feed<br><br>Completed | |
| Data is at risk when being stored. | Project Lead | Data stored on standalone password protected computer. Access restricted to those with issued log on and password.<br><br>All images not required for evidential purposes deleted after 28 days | Accepted | Yes | BWV storage solution adopted for drones Each person with approved access has their own log in and password.<br><br>Completed | |
| Systems cannot delete or anonymise unnecessary | Project Lead | Data stored on standalone password protected computer. With automatic deletion | Accepted | Yes | Solution adopted has automatic deletion | |

| | | | | | | |
|---|---|---|---|---|---|---|
| personal data | | facility. Access restricted to those with issued log on and password.<br><br>All images not required for evidential purposes deleted after 28 days | | | function. Images not selected for retention for deleted. | |
| Incorporation of SAR's footage into the regime for handling information requests | Project Lead | Agreement in place that footage handed to police for policing purposes is subject to Force data handling, security and storage policy.<br><br>Use of Redaction to remove personal data from SAR's. https://ico.org.uk/for-organisations/guide-to-freedom-of-information/refusing-a-request/ | Accepted | Yes | Consider writing into Force Policies<br><br>Decision by Dec 16 | |
| Inappropriate management of data leading to unauthorised disclosure | Project Lead | Effective training of operators in data retention and storage policy | Reduced | Yes | Training in respect of Data Protection Act, covering storage and handling and surveillance camera commissioner s Codes of Practice incorporated into operator's course.<br><br>Force requirement that all staff are familiar with the Force Information Security Policy<br><br>Completed | |

**Force contact point for future privacy concerns:**

Insert contact here: **data.protection@sussex.pnn.police.uk**.

**Step 4 – Review**

The PIA should be reviewed at least annually. A record of this review should be outlined below:

Next review due October 2017.

| Review date | Outcome | Signed: |
|---|---|---|
| | | |
| | | |

.

# Appendix 1

## Data Protection Act Principles

1 Personal data shall be processed fairly and lawfully and, in particular, 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.

2 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.

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

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

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

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

7 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.

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

The links below lead to the:

- ICO CCTV Code of Practice. (Unmanned Aerial Systems (Drones) are included in this on page 29.)
- ICO Conducting PIA code of practice.

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-.pdf

Information Commissioner's Conducting Privacy Impact Assessments code of practice

## Appendix 2

## Surveillance Camera Code of Practice - Principles

System operators should adopt the following 12 guiding 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.

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.

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.

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

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.

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.

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

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.

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

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.

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.

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.

The link below leads to a useful guide to the principles.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/368115/Leaflet_v6_WEB.pdf