Unmanned Aerial System

Type of document Assessment (PIA)	Privacy Impact
Version	4
Registered Owner	Supt Thompson
Author	PC Alan Hincks
Effective Date	18/05/2021
Review Date	27/05/2023
Replace document (if applicable)	
Functional Owner	PC Alan Hincks
Authorised senior user	Tom Thompson (Police) Neil Sadler (Fire)
Data Controller	Chief Constable

Version Control

Version No	Date	Post Holder/Author	Post	Reason for issue
0.1	11/10/2016	Technical Support Joint Operations Team (D. Dodwell)	JOT	Draft
0.2	19/12/2016	Technical Support Joint Operations Team (D. Dodwell)	JOT	Minor amendments following ICO consult
0.3	19/12/2016	Technical Support Joint Operations Team (D. Dodwell)	JOT	Formatting and adding of a risk register
1.0	18/01/2017	Technical Support Joint Operations Team (D. Dodwell)	JOT	Final

1.1	25/04/2018	Technical Support Joint Operations Team (D. Dodwell)	JOT	
1.2	29/05/2018	Technical Support Joint Operations Team (D. Dodwell)	JOT	Changes to reflect the GDPR
2	1/07/2018	Technical Support Joint Operations Team (D. Dodwell)	JOT	Final
3	24/08/2019	Technical Support Joint Operations Team (D. Dodwell)	JOT	Final minor amendments and changes to terminology
4	18/05/2021	Joint Operations Team Air Safety Manager (A. Hincks)	JOT	Review/Update owner

1. Introduction

1.1. Northamptonshire Police (NP) and Northamptonshire Fire and Rescue Service (NFRS) will be operating an Unmanned Aerial System (UAS) at spontaneous and pre-planned events/Incidents. The primary functions are to provide operational support for officers dealing with multi-agency incidents, preventing and detecting crime, assisting scene assessment at large scale fire incidents and in matters involving public safety.

1.2. This Privacy Impact Assessment has been written to explore these issues and in particular to explain:

1.2.1. The key privacy issues and risks and provides an explanation as to how the organisation mitigates them.

1.2.2. The legality behind its use.

1.2.3. The likely operational circumstances when Pilots and observers may use it.

1.2.4. How the Police Force will continue to monitor the use of the equipment and revisit the Privacy Issues and Risks through on-going consultation with its community, together with responding to any national and legislative changes.

1.3. This document should also be viewed in the context of the operations manual that the pilots and observers abide by.

2. Purpose Of Privacy Impact Assessment (PIA)

2.1. Any project or set of new processes that involve exchanging personal information has the potential to give rise to privacy concerns, from the public. This document is a method by which to alleviate any public concerns for the use of this relatively new technology.

2.2. What is meant by privacy?

The Information Commissioner's Office Conducting Privacy Impact Assessments code of practice describes privacy in the following way:

2.2.1. Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion:

2.2.1.1. Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

2.2.1.2. Informational privacy - the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

2.3. The Privacy Impact Assessment (PIA) is a process which helps organisations to anticipate and address the likely privacy impacts of projects, in order that problems can be foreseen and solutions developed to ensure that concerns are addressed appropriately.

2.4. Police Forces, have introduced the use of cameras that are capable of capturing both moving and non-moving images via a UAS operated by qualified pilots and observers. The devices have been used in a number of policing and fire service situations and the aim of undertaking this PIA is to explain the extent of:

2.4.1. their use

2.4.2. their limitations

2.4.3. how any data captured will be processed

2.4.4. analysis of the rights to privacy of citizens and the risks that this could impose on its introduction.

2.5. Finally, this PIA only addresses the application of this equipment for overt policing and fire and rescue operations.

3. What is an Unmanned Aerial System (UAS)?

3.1. The UAS, which this PIA refers to, consists of a small (<20 kg) Quadcopter vehicle, camera, remote control unit and tablet. This system is deployed to provide aerial imagery in the form of both video and pictures. These images if required will be stored on a secure password protected database currently used for normal Force data capture.

4. Why Use an UAS?

4.1. The police have a responsibility to maintain law and order; to protect members of the public and their property, and prevent, detect and investigate crime. They will also, by providing aerial support, assist other agencies in

both, joint operations or when that imagery is required for a sole agency purpose.

4.2. By the introduction of this type of technology, the devices themselves are able to record exactly what is happening and either record or stream that information live to a command post. Their use should be:
  4.2.1. Incident specific
  4.2.2. Proportionate
  4.2.3. Legitimate
  4.2.4. Necessary, and Justifiable.

4.3. The following categories of citizens are likely to be recorded either directly or indirectly by officers during an ongoing incident;
  4.3.1. victims of crime,
  4.3.2. Persons who have been reported as missing
  4.3.3. persons suspected of committing offences
  4.3.4. witnesses of crimes
  4.3.5. In addition, persons, unrelated to any specific interaction between police officers and any of the categories of persons above, may find their activities captured on a UAS video device. To some degree, this is inevitable since a camera lens is non-discriminatory and captures what is seen.

4.4. UAS video will not be routinely recording and monitoring all activity on a continuous basis. To do so would fundamentally breach the privacy of large swathes of the public, who are going about their legitimate lives, as well as the privacy of officers going about their work. This cannot be justifiable from the perspective of proportionality and legitimacy and would breach Data Protection Legislation.

4.5. Added to this, is that current technology is incapable of operating in such a way, principally due to a lack of suitable battery life. In addition, such a practice would require the storing, reviewing and then disposal of large quantities of data.

4.6. The equipment will be used by qualified pilots and observers, and the use will be primarily driven by the incidents and circumstances presented to them or in anticipation of responding to a reported and unfolding incident, or when exercising a specific power.

5. General Operating Procedures

5.1. To reduce duplication, the Northamptonshire Police procedure details the general operating procedures and they have not been reproduced here.

5.2. A set of operational guidance notes has been produced by the police service on the use of the UAS aerial imagery and associated back-office software.

5.3. Any material required to support an on-going investigation or prosecution will be retained as fulfilling a 'policing purpose', and be processed under the Home office/NCPE (2005) Code of Practice Management of Police Information guidance (MoPI) College of Policing (2013) APP on Information

Management as well as the Criminal Procedures Investigations Act 1996 (CPIA). All other material will be automatically erased after 31 days.

5.4. Any information that could be used for future operational learning maybe retained and used as necessary for an unspecified period, however there must be a recognisable and legitimate learning outcome.

5.5. Any information shared with the Crown Prosecution Service for the purpose of determining any advice/charge and then to assist in any prosecution, will be strictly controlled in accordance with the Crown Prosecution Service (2020) The Director's Guidance on Charging 6th Edition.

5.6. In order that aerial imagery evidence is admissible in court, Northamptonshire Police follow the principles contained in the ACPO/Home Office (2007) Digital Imaging Procedure v2.1 and the ACPO (2007) Practice Advice on Police Use of Digital Images.

6. The Law surrounding the use of UAS

6.1. The use by the police of UAS video must be shown to be proportionate, legitimate, necessary and justifiable. This next section explains the various aspects of the legislation and guidance that covers this equipment, and how the Northamptonshire Police will ensure that the rights and privacy of the public are balanced against the law.

6.2. Legality under Common Law

6.2.1. The taking of photographs, and in its wider sense video or sound recordings, is deemed lawful and Common Law does not prevent this activity in a public place. (Lord Collins in Wood v Commissioner of Police for the Metropolis 2009). (Murray v the UK (1995)

6.2.2. European Convention of Human Rights Act 1998

6.2.2.1. For the purposes of the European Convention of Human Rights (ECHR) and the Human Rights Act 1998, it has been determined that a public authority has sufficient Authority in law to justify the use of aerial imagery as above (Wood v Commissioner of Police for the Metropolis [2009] and Murray v the UK [1995]), however use of aerial imagery is viewed as 'an interference' and must always be justifiable. Therefore any actions by the public authority must have a legitimate aim and the use of this equipment must be shown to be proportionate to achieving this. Under this legislation a number of 'Articles', protect the rights of citizens. Some of these Articles are absolute whereas others are 'qualified' and any interference with these is limited.

6.2.2.2. Interference with qualified rights is permissible only if:

6.2.2.2.1. There is a clear legal basis for the interference with the qualified right that people can find out and understand, and

6.2.2.2.2. The Action/Interference seeks to achieve a legitimate aim. Legitimate aims are set out in each article containing a qualified right and they vary from article to article, they include for example, the interests of National Security, the prevention of

disorder or crime and public safety. Any interference with one of the rights contained in articles 8 -11 must fall under one of the permitted aims set out in the relevant article.

6.2.2.2.3. The action is necessary in a democratic society. This means that the action or interference must be in response to a pressing social need and should be assessed by demonstrating evidence of a level of severity or immediacy/unpredictability, and alternatives should have been reviewed.

6.2.2.3. The use of aerial imagery must comply with ECHR, and there are two particular Articles that are critical and most likely to be challenged.

6.2.2.4. Article 8 of the ECHR is the right to respect for private and family life, home and correspondence.

6.2.2.5. Under the legislation, this article is a qualified right and, Police forces are required to consider this article when dealing with recorded images, whether they are made in public or private areas. Accordingly, this assessment looks to address the issues raised by this Article and introduces suitable safeguards, associated with how a Police Force deploys this equipment, in the public and private arena, and then how it deals with the product from any use. Throughout, the principle objective is ensuring that any interference with the rights of parties can only be justified if it is:

6.2.2.6. Necessary

6.2.2.7. In pursuit of a legitimate aim - such as the prevention, investigation and detection of crime, with the necessity test being satisfied by the presence of a pressing social need,

6.2.2.8. In accordance with the law - legal advice has been sought to establish that aerial imagery is in accordance of the law.

6.2.2.9. Article 6 of the ECHR provides for the right to a fair trial.

6.2.2.10. Some images from the UAS have the potential for use in court proceedings whether they provide information that is beneficial to the prosecution or defence. The information will be safeguarded by an audit trail in the same way as other evidence that is retained for court.

6.2.2.11. It must be emphasised that a UAS camera can collect valuable evidence for use in criminal prosecutions, ensure the police act with integrity and transparency and potentially provides objective evidence of controversial events. It offers protection for both citizens and the police. However this justification may be closely scrutinised by a court and it is essential that recordings will not be retained where there is no clear evidence of an offence, unless some other good reason exists for their retention.

6.2.2.12. Users of the UAS must consider Article 8 when recording and must not record beyond what is necessary.

6.2.2.13. Northamptonshire Police will continue to monitor all use of this equipment to ensure that it remains proportionate and undertakes to update this PIA process if their findings warrant any change.

6.2.3. Data Protection Act 2018

6.2.3.1. The Data Protection Act 2018 (DPA) and the General Data Protection Regulations (GDPR) is legislation that regulates the processing of personal data including sensitive personal data, whether processed on a computer, CCTV, stills camera or any other media. Any recorded image and audio recording from any device, which includes aerial imagery, that can identify a particular person or learning about their activities, is described as personal data and is covered by the regulation. The guiding principles of protecting data are contained within the appendix;

6.2.3.2. Northamptonshire Police Force have the responsibility for controlling this information and the Chief Constable is known as the Data Controller for information captured and used within its area, for a policing purpose. If required, a police officer or someone acting within his authority is using a UAS, must be prepared to explain how the capture and processing of any data is compliant with the legal obligations imposed under this Act. However, the Northamptonshire Police Force has clearly identified UAS devices under its control. Therefore, as a general rule, where an officer or representative is in uniform and is clearly identified as a UAS operator this condition would be considered to have been satisfied.

6.2.3.3. In order for the Northamptonshire Police Force to ensure compliance with the regulations, the following has been undertaken:

6.2.3.3.1. a local media campaign to advertise the use of a UAS , using local newspapers and other media and the force website;

6.2.3.3.2. advise the local community-based forums of the use of this technology in the area;

6.2.3.3.3. Ensure users where possible/practicable; announce to the subject(s) of an encounter that video recording is taking place using a UAS.

6.2.3.3.4. The sharing of UAS images with other agencies and the media, and any images will only occur in accordance with the requirements of the Act.

6.2.4. Criminal Procedure and Investigations Act 1996

6.2.4.1. The Criminal Procedure and Investigations Act 1996 introduced the statutory test for disclosure of material to the defence in criminal cases.

6.2.4.2. The Northamptonshire Police Force is able to disclose both used and un-used images and demonstrate that this has been done.

Deletion of any police-generated images (or a third party's images in police possession) prior to their respective retention periods, may amount to a breach of the Act if they are not then available for disclosure. Images that are relevant to an investigation must be retained in accordance with the Code of Practice issued under Section 23 of the CPIA.

6.2.4.3. The ACPO (2007) Practice Advice on Police Use of Digital Images section 1.2 Criminal Justice Disclosure contains further information about this requirement. Police generated digital images should be accompanied by a full audit trail, from the point of capture of the image throughout the whole management process - including when they are passed to the CPS or the defence or if there is any supervised viewing.

6.2.5. Freedom of Information Act 2000

6.2.5.1. The Freedom of Information Act 2000 grants a general right of access to all types of recorded information held by public authorities, which includes digital images recorded by a UAS.

6.2.5.2. The Act does however provide some specific exemptions to the requirements to disclose information.

6.2.6. Protection of Freedoms Act 2012 & the Surveillance Camera Code of Practice

6.2.6.1. Part 2 of the Protection of Freedoms Act 2012 deals with the regulation of CCTV and other surveillance camera technology and introduces the Code of Practice for Surveillance Camera systems. Section 29(6) of the Act provides that this code covers "any other systems for recording or viewing visual images for surveillance purposes". This would include aerial imagery.

6.2.6.2. Northamptonshire Police Force adhere to this code as its content will be relevant when a court is considering whether the use of aerial imagery;

6.2.6.2.1. Complies with Data Protection principles;

6.2.6.2.2. Is prescribed by law for the purposes of Article 8 ECHR; and

6.2.6.2.3. Is a proportionate interference with Convention rights under Article 8(2) ECHR.

6.2.7. Home Office/NCPE (2005) Code of Practice on the Management of Police Information (MoPI)

6.2.7.1. This consists of both guidance and a Code of Practice that directs how the Police Service will handle any data that comes into its possession. Data, which includes information from a UAS.

6.2.7.2. The guidance further states that a Policing Purpose includes:

6.2.7.2.1. Protecting life and property

6.2.7.2.2. Preserving Order

6.2.7.2.3. Preventing the commission of offences

6.2.7.2.4. Bringing offenders to justice

6.2.7.2.5. Any duty or responsibility of the police arising from common law or statute

6.2.7.3. These five purposes provide the legal basis for collecting, recording, evaluating, sharing and retaining police information.

6.2.7.4. The guidance provides a framework on how any data captured by the police can be used and processed. In addition, it details the process to be used by the police service to initially retain information, to review this and to when to ultimately dispose Of data after requisite timescales and circumstances. In addition the College of Policing APP on Information Management contains useful additional information.

7. Data flows

Data is captured in accordance with Northamptonshire Police Force data capture procedures and to avoid duplication is not repeated in this section.

8. Data requests

Subject Access requests to data captured by the UAS will be dealt with in accordance with existing Northants police procedures through the information unit.

9. Public acceptability

9.1. Northamptonshire Police Force sees this element as an essential part in its introduction and use of the UAS. It is critical that the organisation continues to retain the trust and consent of the local community.

9.2. Accordingly, it has completed a communication and consultation programme at the start of its current deployment as per the usual police engagement procedures. It involved different organisations, groups and utilised a variety of communication mediums.

9.3. Although the Force has carried out an engagement exercise it is important to stress that consultation should be ongoing and any lessons learned be reflected in future updates to this document.

9.4. Social Media

9.4.1. Social media will be used to help promote and increase public awareness. Likewise it is envisaged that positive messages from the use of the UAS will be publicised where appropriate.

10. Privacy Issues and risk mitigation

10.1.1. Through the introduction of this type of technology, there might naturally be concerns associated with how any information is being captured, processed and retained by Northamptonshire Police Force. The risk register below details how these risks are controlled.

Privacy Risk	**Privacy Control Measure**
The UAS introduces a new way of providing data to the police force and as such has the potential to be intrusive to privacy	The UAS will only be flown by trained operators following the procedures outlined in this document and in accordance with all

	legislation applicable to flight and data protection.
UAS footage may be shared with other agencies risking data being made available contrary to data protection principles.	When imagery is captured it will be for a specific purpose. The imagery will be held securely on an approved police system and will only be shared when authority is given by a police officer. The information shared will be checked to ensure that sensitive data is managed within data protection principles
How will any information be shared with the Crown Prosecution Service, Defence and the Courts?	Any captured information deemed to be evidential, will be 'protected' by means of downloading and marking the footage as evidential. This remains an integral part of the process. The current system of passing digital images to CJ partners by DVD, or appropriate storage medium, will remain until a workable solution has been created to pass files digitally. Where a Police Force within the region has the capability to pass files electronically already that process will remain.
Non Compliance with legislation	Northamptonshire Police will only deploy this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing social need. At all stages it will comply with the principles of data protection and other legislation outlined above. In the case of the Human Rights Act 1998, there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim as detailed earlier.
Will the handling of any data, change significantly to be of concern?	The data from the UAS will be managed using existing process for data management already in place within Northamptonshire police
Loss of Data through a downed UAS.	NP will only fly the UAS within visual line of sight and in a controlled area. Data will be removed from the camera after each incident/event. This process will reduce the risk of large volumes of data being lost in a case where operators are unable to recover the equipment and data captured. In such a case, the information security officer will be contacted and a review undertaken.

Data loss while streaming live video feeds	Encrypted (COFDM AES 256) password protected link provided. While live streaming is taking place, the imagery will be constantly monitored to ensure that the data is proportionate legitimate and complies with legislation.
Collateral intrusion	Collateral intrusion in this context extends to the capturing of the movements and actions of other persons or property when this equipment is being used. It is inevitable that in some circumstances this will occur, albeit officers are trained to ensure that wherever possible, the focus of their activity is on the person subject of the officer's attention. The collection of collateral intrusion will be kept to a minimum. Operators are given instruction and guidance on data protection.

11. APPENDICES Data Protection Principles

The GDPR sets out seven key principles:

1. Lawfulness, fairness and transparency
    - processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
2. Purpose limitation
    - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')
3. Data minimisation
    - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. Accuracy
    - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. Storage limitation
    - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')
6. Integrity and confidentiality (security)
    - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
7. Accountability
    - "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."