OFFICIAL

Data Protection Impact Assessment: Remotely Piloted Aircraft Systems

Law Enforcement Processing only

Control Sheet

(Please note this form is unprotected to allow processing by Information Management. To manually check the boxes **right click** on the tick box choose properties from the drop down and select 'check')

URN (to be complete by Information Assurance)	20-189 (Annual Review)
Date Approved	16 February 2022 (Annual Review complete)
Version Number	2.0
Document Status	Approved
Author	Inspector [redacted]
Strategic Information Asset Owner	ACC Williams
Transformation Project	Yes ☐ No ☒
Is this project a pilot?	Yes ☐ No ☒
Date on which the proposed processing is to start (if known)	Existing processing – DPIA review

Revision History

Version	Date	Summary of Changes
0.1	03.8.18	Initial Draft DPIA Pt 1 Law enforcement
0.2	15.08.18	Initial draft amendments/ clarification
0.3	16.08.18	IA updates Pt 1
0.4	24.10.18	Parts 2 - 6 entered
0.5	07.11.18	IA updates Pts 1 - 6
0.6	07.12.18	Author update
0.7	12.12.18	IA update
1.0	01.02.19	V1.0 created following final IA review
1.1	08.01.20	Annual review of IA and transfer to new template
1.2	31.01.20	Created to reflect changes by IA
1.3	02.03.20	Update by author following IA feedback
1.4	12.03.20	Updates by IA – 2020 review approved

OFFICIAL

1.5	08.03.21	Annual review draft by PI [redacted] / PS [redacted]
1.6	11/03/21	IA Updates
1.7	14/05/21	IA and author updates
1.8	10.2.22	Consultation completed. IA and author updates.
1.9	16/02/22	Created by IA to capture updates (email addresses) and reflect approval for this annual review.
2.0	08/04/22	Updated by IA to reflect the development of the Code of Practice

Consultation History

Version	Date	Name	Designation
1.7			Information Management
1.7	20.12.21	[redacted]	Scottish Police Authority (SPA)
1.7	20.12.21	[redacted]	Scottish Police Federation (SPF)
1.7	9.7.21	[redacted]	Crown Office Procurator Fiscal (COPFS)
1.7	23.9.21	[redacted]	Scottish Institute for Policing Research (SIPR)
1.7	12.8.21	[redacted]	Scottish Human Rights Commission
1.7		No feedback provided	Information Commissioners Office (ICO)
1.7		No feedback provided	Privacy International
1.7	29.9.2021	[redacted]	Law Society Scotland

OFFICIAL

Part 1 – Determining whether the proposed processing of personal data for law enforcement purposes is likely to result in a high risk to the rights and freedoms of the data subject.

The guidance notes must be read before answering the questions.

Once completed, this part must be submitted to Information Assurance (IA) to decide whether the proposed processing is high risk. (Refer to the definition of law enforcement purposes in Appendix 1 of the Guidance Notes.)

Part 1 Section 1 - General

1.1.1 Does the project involve the processing of personal data? (Refer to the definition of personal data in Appendix 1 of the Guidance Notes).	
☒ Yes ☐	
Click here to enter text	
1.1.2 Who is the Lead/Manager/Senior Responsible Owner for the project?	
Name:	[redacted]
Designation:	Inspector, Air Support Unit
Contact details:	
1.1.3 State who has responsibilities for the personal data. (Refer to Note 1 of the Part 1 Guidance Notes.	
Strategic Information Asset Owner	
Name:	Mark Williams
Designation:	ACC Operations
Contact details:	[redacted]@scotland.police.uk
Tactical Asset Owner	
Name:	[redacted]
Designation:	Superintendent, Head of Specialist Services, OSD
Contact details:	
1.1.4 Provide a summary of the project. (This **must** be done in accordance with Guidance Note 2 of the Part 1 Guidance Notes)	
To enhance the current police air support capability, Remotely Piloted Aircraft Systems (RPAS) (known also as drones) are operationally available at Aberdeen, Glasgow and Inverness. Police Scotland has 7 RPAS platforms (3 x DJI M210 and 4 x DJI Phantom). Both RPAS types can be deployed operationally, however the M210 platforms are used primarily in the search for missing persons but will also be deployed to a variety of policing incidents, operations and events, where appropriate, as well as training, research and development.	

OFFICIAL

RPAS are only deployed operationally for a legitimate policing purpose where it is necessary and proportionate.

Whilst not capable of undertaking some of the tasking already carried out by the PS helicopter, RPAS has been deployed at variety of policing incidents. They are suitable for the following deployments:-

Searches
- Missing persons
- Suspect persons
- Evidence
- Property

Critical Incident Response
- Firearms
- Public Order
- Major Incident

Post Incident Investigation
- Scene overview and situational awareness for emergency services
- Aerial images for safety, analysis, strategy

Crime Scene Analysis Imagery
- Evidential imagery for criminal proceedings
- Road Traffic Collisions
- Serious Crime

Divisional initiatives supporting the local policing plan
- Aerial imagery for event planning
- Public safety
- Officer safety
- Public confidence

The DJI Phantom platforms are predominantly utilised for officer training, however will be deployed to undertake photographic tasks where appropriate.

All RPAS operations can be conducted both day and night and in accordance with aviation law and regulated by the CAA (Civil Aviation Authority). The RPAS operation as a whole sits within the Air Support and as such has an accountable manager (Inspector of Air Support Unit). An operational safety case and operations manual are held by Police Scotland which is reviewed annually by the CAA.

Each RPAS is operated by two police officers. Twelve officers in total have been trained around Scotland. They have been trained by National Air Traffic Services to pilot the aircraft and are certified to NQE CAA standard. Officers are trained to operate both RPAS types which are within the 0-20kg category.

RPAS is fitted with a dual sensor camera system which includes daytime video (EO) and thermal image (IR) camera sensors. Imagery is transmitted from the camera to the ground based controller which has a screen and is viewed by the police officer operating it. [redacted] It should be noted that the camera sensors attached do NOT have facial recognition capability.

OFFICIAL

Similar to the Police helicopter, RPAS can act as an airborne command and control platform providing an overview of an incident. This provides Police Commanders with enhanced situational awareness allowing them to make informed decisions in response to an incident and how to effectively deploy ground resources.

All RPAS activity is overt and high profile. RPAS are not deployed covertly. However in the event of an incident which requires an immediate response to a threat to life or national security, then RPAS may be considered as a covert option. Any such decision would be done under strict adherence to Regulation of Investigatory Powers (Scotland) Act 2000.

For missing persons tasking, RPAS is used to search large open areas for one person or a small group of people for example.

In terms of recording and retaining imagery, this would be carried out for police event planning, criminal investigation and evidential purposes ONLY.

Images of a crime scene or related to crime or incident are treated as productions. In the investigation of serious crime these may be retained with crime records and are subject to rules as outlined in the Police Scotland Records Retention Standard Operating Procedure.

RPAS have the ability to downlink and stream live video feed from the camera sensor via the camera operators control unit. [redacted] This is then distributed to a limited number of, password protected, viewing clients within the Police Scotland network. No personal data is shared with the manufacturer or supplier of the equipment.

RPAS platforms have completed a total of 577 flying hours since 2018. This included testing, acceptance and training flights prior to operational use.

Since May 2019, when RPAS was launched operationally, the Air Support Unit has deployed RPAS 194 times in support of operational policing around Scotland. The majority of these deployments have been in support of missing person searches, but also includes crime scene aerial imagery/ searches during murder investigations, aerial imagery for fatal fires, and serious road traffic collisions.

All RPAS operational deployments are conducted by highly visible uniformed police officers operating within a controlled area not accessible by the public. Prior to deployments (where applicable) Police Scotland will conduct public engagement e.g. Local policing officers conducting door to door enquiry informing householder's of pending RPAS activity in their local area, this affords residents the opportunity to ask questions and for officers to address concerns, Police Scotland RPAS information leaflet being distributed, use of Social Media to inform the public of RPAS deployment reaches a national audience. These methods have been employed and have met with positivity from the public. No negative feedback has been recorded by Police Scotland for RPAS deployment. The overarching feeling encountered by Police Scotland officers has been one of positivity and curiosity with regards to the technology.

It is envisaged that public engagement will not always be possible on the rare occasion where spontaneous critical incidents are encountered and for matters of national security.

In addition to the operational deployment, an RPAS will be utilised at Glasgow for research and

OFFICIAL

development. This collaborative working, with partners such as Glasgow University, University of West of Scotland, CENSIS and Thales, will explore the evolving technology of aircraft systems and sensor equipment for future emergency service use and wider industry users. No personal data will be processed for this part of the project, it concerns only the development of the equipment.

In January 2021, PS referred its use of RPAS to an Independent Ethics Advisory Panel (IEAP) to consider use of RPAS for policing incidents and operations other than missing person investigations. The IEAP was chaired by a Sheriff and consisted of 12 panel members from a diverse variety of organisations representing academia, industry, public sector, private sectors and 3rd party sector agencies. Notably, several of the panel members are renowned internationally and received recognition for their expertise and contributions to human rights.

In conclusion the panel emphasised the importance of PS community engagement prior to RPAS deployment with the relevant community or communities likely to be close to, or affected by RPAS deployment, and the continued need to secure public confidence in the decision making framework. The panel also suggested further ways in which PS could engage with the public which reflected practices already in place.

PS RPAS operations have come under significant scrutiny recently. PS will continue to engage with the communities of Scotland and stakeholders to ensure transparency and provide reassurance around RPAS acitivity and increase confidence in policing.

The original DPIA for this project was approved in February 2019 and it is reviewed on an annual basis.

Part 1 Section 2 – The purpose of the processing

1.2.1 What is the reason you want to process the data? If in Q1.1.4 you have covered in full the reason you want to process the data, then please copy and paste the relevant sections here.
To record and retain aerial imagery for the investigation, detection and prosecution of criminal offences. e.g. (1) Search for a vulnerable missing person in a large open area - body found and images obtained for investigation/ inquiry. e.g. (2) Large scale disorder outside football stadium involving 100s of people. Imagery used to identify those involved and subsequent criminal proceedings. e.g. (3) Armed police officers deployed to residential dwelling to provide initial armed response to an individual with access to firearms. Siege type incident ensues and a RPAS is deployed to contain the dwelling curtilage/ street and monitor and records police response. Footage used in subsequent criminal proceedings. e.g. (4) Aerial images obtained of the scene of a serious/ fatal RTC to assist in the collision investigation and subsequent criminal proceedings. e.g. (5) Imagery obtained to assist with operational planning
1.2.2 What is the intended outcome for the individuals whose data you propose to process?
To be identified for the purposes of prosecution or assistance in the safeguarding of vulnerable persons.
1.2.3 What are the expected benefits for Police Scotland?

OFFICIAL

Aerial imagery recorded and retained to assist in the investigation, detection and prosecution of criminal offences.

1.2.4 What are the expected benefits for society as a whole?

Identification and prosecution of offenders and deployment of relevant and necessary Police resources. This in turn will likely lead to a reduction in police time and significant resources investigating these incidents.

Part 1 Section 3 – Nature of processing

1.3.1 Has the Information Security (ISM) Manager been consulted: This should be done at the outset of any project – iso@scotland.pnn.police.uk

☒ Yes

☐ No – if not, this must be done immediately.

☐ Not applicable – state below why there is no requirement to consult the ISM.

Click here to enter text

1.3.2 Have the asset owners of any related systems been consulted?(e.g. IT, paper, video etc.)

☒ Yes – If so, provide details.

☐ No – state below at what stage you intend to consult.

DPIA will be shared with relevant parties which include, but not limited to ICT as part of consultation process.

1.3.3 What will the classification of the data be under the Government Security Classification (GSC)? (GSC SOP)

Official ☐ or

Official Sensitive ☒ (NB Official Sensitive **must** be accompanied by handling instructions)

Named Recipients Only ☐ Police and Partners ☒ Police Only ☐

1.3.4 Will any processing be done via an internet/cloud based system?

☐ Yes – Provide the details below.

☒ No

1.3.5 Will Police Scotland be processing the personal data jointly with another organisation? (Refer to the definition of controller in Appendix 1 of the Guidance Notes) If so, documentation will be required to regulate the relationship.

☐ Yes – provide details of the other organisation, their Data Protection Officer (DPO) and the exact role of the other organisation in the processing of the data.

☒ No

OFFICIAL

Click here to enter text

1.3.6 Will another organisation be processing any of the personal/sensitive data on behalf of Police Scotland? (Refer to the definition of processor on page 6 of the Guidance Notes). If so, a contract will be required to regulate the relationship.

☐ Yes – provide details of the other organisation, their Data Protection Officer (DPO) and the exact role of the other organisation in the processing of the data.

☒ No

Click here to enter text

1.3.7 Will the processing involve new technology? i.e. technology that is new to Police Scotland.

☐ Yes – If so, give brief overview of it below. If this has been included in the summary of the project, please copy and paste the relevant sections below.

☒ No

1.3.8 Will the processing be done in any novel or unexpected ways? E.g. machine learning or artificial intelligence.

☒ Yes – If so, give brief overview of it below. If this has been included in the summary of the project, please copy and paste the relevant sections below.

☐ No

Police Scotland has collaborated with University of West of Scotland to design and develop a software package which utilises artificial intelligence (AI) and assist the RPAS camera sensor to identify a human form during area searches for missing persons. This AI technology will be installed on a mobile phone device connected to the RPAS controller. The software has been developed through machine learning. This does not alter the way in which the data is recorded or processed. This is NOT facial recognition. It is an effective and efficient tool reducing the cognitive burden of the camera operator during interrogation of live imagery. Please see link for more details:

https://www.bbc.co.uk/news/uk-scotland-50262650

OFFICIAL

Part 1 Section 4 – Scope of the processing – What the processing covers

1.4.1 What categories of data subject are involved? (Please select all applicable)
☒ Victims ☒ Witnesses ☒ Suspect ☒ Accused ☒ Person convicted on an offence ☒Children or vulnerable individuals – provide details below ☐ Other – provide details below
Air support search for missing or vulnerable persons.
1.4.2 What is the source of the personal data? (Please select all applicable)
☒ Victims ☒ Witnesses ☒ Suspect ☒ Accused ☒ Person convicted on an offence ☒Children or vulnerable individuals – provide details below ☐ Other (e.g. data already held in other Police Scotland systems, partner agencies etc.) - provide details below
Data may be processed via camera sensor during the search for missing or vulnerable persons.
1.4.3 List all categories of personal data to be processed. This should also include the types of information if appropriate, e.g. videos, pictures, audio files. (Refer to the definition of personal data in Appendix 1 of Guidance Notes)

OFFICIAL

Videos, still photographs.

1.4.4 Does this project involve processing sensitive data? If so, tick all categories of sensitive data to be processed.

☒ Race
☒ Ethnic origin
☒ Political opinions
☒ Sex Life
☒ Religion
☒ Philosophical beliefs
☒ Trade Union membership
☐ Genetic data
☐ Biometric data
☒ Sexual orientation
☒ Health
☐ Criminal conviction data
☐ None

1.4.5 Will the personal/special category/criminal conviction data be shared with anyone?

☒ Yes – provide details below
☐ No

Whilst the intention is to capture footage/images of those committing crime or assisting in the investigation of vulnerable persons, it is recognised that by the nature of filming, other information may be captured inadvertently such as protests from any of the above categories. This footage may be shared with other law enforcement partners such as the crown office for prosecution. Terrain imagery that is not linked to personal information may be shared with the University of West of Scotland during collaboration of development of sensor technology

1.4.6 Does the proposed processing involve the collection of data not previously collected by Police Scotland?

☐ Yes – provide details below
☒ No

Click here to enter text

1.4.7 Will the personal/sensitive data be fully identifiable, pseudonymised or anonymised? (Refer to Guidance Note 3 of the Part 1 Guidance Notes)

☒ Fully identifiable
☐ Pseudonymised – provide details of how this will be done, and at what stage in the process
☐ Anonymised – provide details of how this will be done, and at what stage in the process

OFFICIAL

Click here to enter text
1.4.8 Does the proposed processing involve any alignment or combining of data sets?
☐ Yes – provide details below ☒ No
Click here to enter text

1.4.9 How many individuals will be affected by the proposed processing, or what is the percentage of the population affected?
This is difficult to say and will depend on the specific task that RPAS has deployed to. The overwhelming majority of tasking will be overt and operated by highly visible uniformed police officers at a static and public point. If operated in public areas it is not known how many persons will be there. Prior to deployments (where applicable) Police Scotland will conduct public engagement e.g. Local policing officers conducting door to door enquiry informing householder's of pending RPAS activity in their local area, Police Scotland RPAS information leaflet being distributed, use of Social Media to inform the public of RPAS deployment.
1.4.10 What is the geographical area involved? e.g. one division, a number of divisions, whole of Scotland. If this is not to cover the whole of Scotland, name the divisions/areas involved.
The whole of Scotland

Part 1 Section 5 – Context of the processing – The wider picture including internal and external factors which might affect expectations or impact

1.5.1 Are there prior concerns internally over this type of proposed processing, or known security flaws?
☐ Yes – provide details below. This must be addressed in the risk assessment ☒ No
Click here to enter text
1.5.2 Describe any relevant advances in technology or security

OFFICIAL

Police Scotland has collaborated with University of West of Scotland to design and develop a software package which utilises artificial intelligence (AI) and assist the RPAS camera sensor to identify a human form during area searches for missing persons. This AI technology will be installed on a mobile phone device connected to the RPAS controller. The software has been developed through machine learning. This does not alter the way in which the data is recorded or processed. This is NOT facial recognition. It is an effective and efficient tool reducing the cognitive burden of the camera operator during interrogation of live imagery.
1.5.3 Are there any current issues of public concern in the area of the proposed processing? If so, provide details.
☒ Yes – provide details below. This must be addressed in the risk assessment. ☐ No
Following submission of a report to the SPA in November 2020, a number of concerns were raised by the SPA and a Scottish Government Justice Sub Committee in relation to extent of proposed use of RPAS, privacy, ethics and human rights. These concerns have been comprehensively addressed by Police Scotland through referral to an Independent Ethics Advisory Panel, significant lettered correpsondance, parliamentary public consultation and an evidence hearing. A revised evaluation report was subsequently presented to the SPA in March 2021 which provided further clarification on the concerns. To date PS has not received any complaints form members of the public re use of RPAS.
1.5.4 What relevant codes of practice have been considered and complied with? (Refer to Guidance Note 4 of the Part 1 Guidance Notes)
Air Navigation Order 2016, CAA Publication CAP 722 Remotely Piloted Aircraft Systems (RPAS) Code of Practice

This form should now be sent to the Information.Assurance@scotland.pnn.police.uk .

It will be returned to you within 5 working days with a decision as to whether the proposed processing is high risk.

Once you receive the response you should then complete Part 2 of this DPIA (which will be sent to you from Information Assurance (IA) with the response to Part 1) and send it to Information.Assurance@scotland.pnn.police.uk

Law Enforcement DPIA Part 2– Assessment of legality, governance and risks

Name of Project: Remotely Piloted Aircraft Systems

URN 20-0189

OFFICIAL

The guidance notes must read before answering the questions. Once completed, this part must be submitted to Information.Assurance@scotland.pnn.police.uk to assess and agree sign off of this DPIA.

Part 2 Section 1 – Assessment of Necessity and Proportionality – The Data Protection Principles and other relevant sections of the Data Protection Action 2018 (DPA 2018)

1st Principle – Lawful and fair. DPA Section 35 and Schedule 8

2.1.1 Is the processing based on consent? If so, further action will be required to comply with the legislation regarding consent.
☐ Yes – explain below why consent is necessary for the purposes of the proposed law enforcement processing ☒ No
No. Processing (imagery) is not based on consent and is strictly necessary for law enforcement purposes. The imagery obtained will be best evidence in support of criminal justice proceedings. The processing is necessary under the Police Fire & Reform (Scotland) Act 2012 – Section (20) Constables: general duties- (1)It is the duty of a constable— (a)to prevent and detect crime, (b)to maintain order, (c)to protect life and property, (d)to take such lawful measures, and make such reports to the appropriate prosecutor, as may be needed to bring offenders with all due speed to justice, Section (32) Policing principles: The policing principles are- (a)that the main purpose of policing is to improve the safety and well-being of persons, localities and communities in Scotland, and (b)that the Police Service, working in collaboration with others where appropriate, should seek to achieve that main purpose by policing in a way which— (i)is accessible to, and engaged with, local communities, and (ii) Promotes measures to prevent crime, harm and disorder.
2.1.2 Does the processing involve the processing of sensitive data? Tick all that applies (See your response to Q1.4.4 in Part 1 of this DPIA)

OFFICIAL

☒ Race	☒ Trade Union membership
☒ Ethnic origin	☐ Genetic data
☒ Political opinions	☐ Biometric data
☒ Sex Life	☒ Sexual orientation
☒ Religion	☒ Health
☒ Philosophical beliefs	☐ None – go to question 2.1.4 below

2.1.3 To process sensitive data for a law enforcement purpose at least one of the following (or another Schedule 8 condition not listed below) must be satisfied. The Schedule 8 conditions must be read in full before completing this question. Check all that apply and provide further details below as to why each applies. Schedule 8 of DPA 2018 (Refer to Guidance Note 1 of the Part 2 Guidance Notes)

☐ The individual has given consent to the processing

The processing:

☒ is necessary for the exercise of a function conferred on a person by an enactment or rule of law **and** is necessary for reasons of substantial public interest

☐ is for the administration of justice

☐ is necessary to protect the vital interests of an individual

☒ is necessary for the safeguarding of children and of individuals at risk

☐ relates to personal data manifestly made public by the data subject

☐ Other Schedule 8 condition – Provide details below

The following Schedule 8 conditions apply to this processing:

1(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law **and** (b) is necessary for reasons of substantial public interest. This function is defined by Sections 20 and 32 of the Police and Fire Reform (Scotland) Act 2012 which outline the duties of a constable and the policing principles, namely it is the responsibility of Police Scotland to protect life and property and improve the safety and wellbeing of persons, localities and communities in Scotland. To do so is substantially in the public interest and will require Police Scotland to process sensitive personal data using RPAS on occasion.

(2) Administration of Justice. Evidence, including sensitive personal data, captured by RPAS will assist in the successful reporting and prosecution of offenders.

(4) Safeguarding of Children and Individuals at Risk. Sensitive data processed as result of a RPAS deployment could form part of a wider assessment of a situational vulnerability being experienced by a child or adult at risk to allow appropriate support to be provided to them.

2nd Principle – Specified, Explicit and Legitimate – DPA Section 36

2.1.4 Is the personal data to be used for the purpose for which it was first gathered?

OFFICIAL

☒ Yes ☐ No – State below the purpose for which it was gathered, and the new purpose	
Click here to enter text	

3rd Principle – Adequate, Relevant and Not excessive – DPA Section 37

2.1.5 What assessment has been made to ensure that the personal data being processed is adequate, relevant and not excessive in relation to what is necessary for the purpose for which they are gathered?
The RPAS will only be deployed, subject to operational availability, on receipt of suitable taskings from the Control Room or other business area. In the majority of cases no imagery will be recorded. If the imagery requested is for evidential purpose e.g. criminal justice proceedings then it is best evidence and relevant. If it is obtained for intelligence purposes then a full assessment will be made along with rules and guidance under RIPSA 2000, where applicable.

4th Principle – Accurate and kept up to date where necessary – DPA Section 38

2.1.6 How will the accuracy of data be checked?
N/A - the data being processed is imagery (still or video) and there are no accuracy issues.
2.1.7 What process will be in place to keep it up to date where necessary?
N/A.
2.1.8 There must be a functionality or procedure to distinguish between fact and opinion. How will you ensure that this is done? If this cannot be done, please explain why.
N/A.

2.1.9 How will you ensure that there will be a clear distinction between personal data relating to different categories of data subjects? E.g. victims, witnesses, accused etc. If this cannot be done, please explain why.
All data is regularly managed and reviewed by Air Support Unit supervisors. The backend system used to comply with CAA regulations and record details of all RPAS activity as outlined in Q1.1.4 will cross refer details of the task and what data has been captured and for what purpose. The narrative section of the flight log will contain personal data and differentiate between different categories of data subject. This information will only be cross referred if imagery has been obtained. Only one entry is created on the Flight Logging System for each flight.
2.1.10 What steps will be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes? DPA Section 38(4) and (5) refers

OFFICIAL

Section 38(4) & (5) of the DPA requires that all reasonable steps must be taken to ensure that inaccurate, incomplete or out of date personal data is not transmitted or made available for any law enforcement purpose. On the occasions that data is recorded, it is reviewed by Air Support Unit supervisors before transmission to an SIO or requesting officer.

5th Principle – Not kept longer than necessary – DPA Section 39

2.1.11 How long will the personal data be retained?
No imagery is retained by the ASU other than images recorded for research and development, and evidential images related to crime. Research and development work is conducted in association with University of West of Scotland, this imagery contains personal data of police officers only who have consented to the filming and not imagery of members of the public. Images related to crime are subject to rules as outlined in the Police Scotland Records Retention Standard Operating Procedure.
2.1.12 Is the personal data covered by the existing Police Scotland Record Retention SOP?
☒ Yes – Quote the relevant section of the SOP below ☐ No – The records manager must be consulted to determine the relevant retention period and the SOP and this DPIA updated.

OFFICIAL

Operational Support Services - Air Support (current V4.00 Page 85)

OSS-001, OSS-002 & OSS-003 will apply;
Incidents requiring Helicopter Assistance – As per crime list
Accidents Involving Helicopter – Archive
Record of Flying Hours – Current year + 1

Crime and Productions

CRP-001 onwards (current v4.00 Pages 22 onwards)

Serious Crime Enquiry (unresolved) – Retain until case resolved
Serious Crime Enquiry (resolved) – Current year + 12
Standard Crime Enquiry (Both resolved and unresolved) – Current year + 6

References to the Helicopter in the Record Retention SOP can also be read as RPAS but this should be updated when the Record Retention SOP is next updated.

2.1.13 The system must be able to weed and delete a) individual records and b) bulk records. How will you ensure that this can be done? e.g. manual intervention, automatic deletion etc.

Once the data captured has been securely transferred from SD card to CD the data will then immediately deleted from the SD card and the card reformatted.

Once the CD containing the data has been forwarded to the reporting officer/ enquiry officer/ SIO it shall be their responsibility to ensure the CD is logged as a production or deleted in line with existing Record Retention schedules.

The flight logging system maintained by the Air Support Unit to record details of RPAS flights for CAA purposes is weeded after current year plus one.

2.1.14 If the data is to be retained after the retention period, e.g. for statistical purposes, how will it be anonymised?

There is no requirement to keep data beyond the retention period.

2.1.15 What processes will be in place to ensure the data is securely destroyed/deleted?

Data will be deleted immediately from the SD card once it has been transferred to CD. This will be a standard post flight check.

OFFICIAL

6th Principle – Security/Security of processing – DPA Sections 40 and 66 – Technical or organisational measures in place to ensure protection of the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage and Obilgations relating to security, respectively.

2.1.16 If in Part 1 you stated that you had not consulted with the Information Security Manager (ISM) has this now been done:
☐ Yes – and advice reveived ☐ No – explain below why this has not yet been done ☒ Not applicable
Click here to enter text
2.1.17 On which risk register will the information be recorded? If it is already on a risk register, please state which.
N/A.
2.1.18 What processes will be in place to determine who will have access to the data/system?
Only ASU personnel will have access to the data [redacted]. Imagery captured via sensor is then transferred to CD and forwarded to client or deleted.
2.1.19 How will access to the system be granted and removed?
Access granted as per post/ role permissions.
2.1.20 What level of security clearance (i.e. vetting level) will be required to access the system? Vetting SOP. Advice regarding this can be also obtained from the ISM/Vetting Unit.
Recruitment Vetting
2.1.21 What data protection/security training will users, processors, external contractors etc. receive, before gaining access to the system?
Relevant online training will be available for Police Scotland officers and staff via the Moodle application on Data Protection / UK GDPR and they are required to undergo annual refresher training.
2.1.22 Confirm you will you have a SyOps/procedure manual/SOP etc. to detail the above?
☒ Yes – state below which of the above. ☐ No – state below, why not.
RPAS SyOps Oerations Manual Operating Safety Case

OFFICIAL

Air Support National Guidance RPAS Code of Practice
2.1.23 What technical controls will be put in place to protect data at rest, from compromise? Check all that apply.
☒ Encryption ☒ Role Based Access Control

2.1.24 How will information be protected in transit?	
☐ Secure email	☐ Encryption
☐ Egress	☒ Other – Provide details below
Transferred by Police officers from SD card to CD	
2.1.25 Explain how loss of data at rest, will be prevented in case of a business continuity incident/disaster recovery. e.g. Business Continuity Plans, backups and frequency, resilience, parallel systems etc.	
Data not retained by ASU.	

Part 2 Section 2 – Information Sharing

2.2.1 Is any of the data being processed to be shared with third parties? i.e. outwith Police Scotland
☒ Yes – state below which 3rd parties. ☐ No – go to question 2.3.1.
Data which does not contain personal information of members of the public, terrain imagery, may be shared with University of West of Scotland during collaboration of development of sensor technology.
2.2.2 If the information is to be shared with third parties, are there Information Sharing Agreements (ISAs) already in place with these third parties?
☒ Yes – agreement(s) in place – Give details below
☐ Not yet – agreement(s) required
☐ No – none required. If not required, state the reason.
Letter of agreement signed by Supt, Head of Specialist Operations

Part 2 Section 3 – Measures contributing to the rights of the data subjects

Subject Access Requests (SARs) – DPA Section 45

OFFICIAL

2.3.1 How will you ensure that the personal data will be available to Information Management for the processing of SARs?
The UK GDPR and the Data Protection Act 2018 strengthen the rights of individuals, as data subjects, in relation to the personal data that Police Scotland holds about them. If an individual wishes to exercise this right, Article 15 of the UK General Data Protection Regulation and section 45 of the Data Protection Act 2018 provide a right of access to the information Police Scotland holds about them. Individuals can submit a subject access request by emailing: dataprotectionsubjectaccess@scotland.police.uk The Air Support Unit or the appropriate Division that holds the data will work with Information Management, who process such requests as a statutory obligation, and respond accordingly subject to certain restrictions. For example, restricting individuals rights may be necessary to protect the rights and freedoms of third parties or to avoid prejudicing the prevention and detection of criminal offences. Data capture will be cross referenced on the ASU flight logging system to assist with subject access requests.

Right to rectification, erasure and restriction – DPA Section 46, 47, and 48

2.3.2 How will you ensure that the personal data can be corrected, deleted or the processing restricted if required, in response to an individual's rights request?
The UK GDPR and the Data Protection Act 2018 strengthen the rights of individuals, as data subjects, in relation to the personal data that Police Scotland holds about them. Concerning this right, the Air Support Unit or the appropriate Division that holds the data will work with Information Assurance, who process such requests as a statutory obligation, and respond accordingly. The above right is subject to exemptions that we may apply, for example if data is being processed for law enforcement purposes or under a legal obligation.

Part 2 Section 4 – Other legal requirements

Auditable Logging – DPA Section 62

2.4.1 The system must create an auditable record (or log) each time a user does any of the following to the personal data. Please confirm or otherwise that the proposed system will do this. This is a legal requirement. If these requirements cannot be met before the system goes live, the system will not be accredited.
a) Collection – the log must record • what data was collected/input • the identity of the individual who updated the system with the data • the date and time the system was updated ☒ Yes – the system will record an auditable record of all of the above ☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of the DPIA.**

OFFICIAL

Click here to enter text
b) Alteration – the log must record: • the data that was altered • the identity of the individual who altered the data • the date and time the data was altered ☒ Yes – the system will record an auditable record of all of the above ☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**
Click here to enter text
c) Consultation (accessing/viewing) – the log must record • what data was consulted • the reason for the consultation • the identity of the person who consulted it • the date and time of the consultation ☒ Yes – the system will record an auditable record of all of the above ☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**
Click here to enter text

d) Disclosure (including transfers) – the log must record: • the information that was disclosed • the reason for the disclosure • the date and time of the disclosure • the identity of the person who made the disclosure • the identity of the recipients of the data ☒ Yes – the system will record an auditable record of all of the above ☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**
Click here to enter text

OFFICIAL

e) Combining with other data – the log must record:

- the data which was combined
- the identity of the individual who combined the data
- the date and time of the combination

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

Click here to enter text

f) Erasure/weeding – the log must record:

- the fact that a specific record was accessed
- that data was erased/weeded
- the identity of the individual who erased/weeded the record
- the date and time of the erasure/weeding

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

Click here to enter text

Data transfers outwith the UK – DPA Sections 72 to 78 (Refer to Guidance Note 2 of the Part 2 Guidance Notes)

2.4.2 Will the data be held in or transferred to a country within the EU but outwith the UK?

☐ Yes – state below which country/countries below

☒ No – go to question 2.4.5

Click here to enter text

2.4.3 For what purpose is the data held in/transferred to the country/countries listed above? Include the legislation which governs the transfer of the data.

OFFICIAL

Click here to enter text
2.4.4 What processes will be in place to ensure the data is adequately protected? This should include the means used to transfer the data, who will have access etc.
Click here to enter text
2.4.5 Will the data be held in or transferred to a country outwith the UK and the EU?
☐ Yes – state below which country/countries below ☒ No – go to question 2.5.1
Click here to enter text
2.4.6 For what purpose is the data held in/transferred to the country/countries listed above? Include the legislation which governs the transfer of the data.
Click here to enter text
2.4.7 What processes will be in place to ensure the data is adequately protected? This should include the means used to transfer the data, who will have access etc.
Click here to enter text

Part 2 Section 5 – Other privacy legislation

2.5.1. Does the project involve the use of powers within any of the following? Check box as appropriate
☐ RIPA 2000 ☒ RIP(S)A 2000 ☐ IPA 2016 ☐ None of the above
2.5.2 If any of the above apply, provide the relevant sections of the legislation
Whilst the majority of deployments will be overt, due to an imminent threat to life or national security, for example, there may on occasion when the RPAS is used covertly when Section

OFFICIAL

6(10), Sect 26(9)(a) and Sect 71 RIP(S)A 2000 will apply. The Investigatory Powers Act has been reviewed and will not impact the operational deployment of RPAS.

Human Rights Act 1998

2.5.3 Article 2 – Right to Life **Does the proposed process involve new or existing data processing that adversely impacts on an individual's right to life?** Schedule 1 of the Human Rights Act (HRA) 1998
☐ Yes – provide details below ☒ No
Click here to enter text
2.5.4 Article 3 – Prohibition of torture **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right not to be subjected to torture or inhuman or degrading treatment or punishment?** Schedule 1 of the Human Rights Act (HRA) 1998
No.
2.5.5 Article 4 – Prohibition of slavery and forced labour **Does the proposed processing involve new or existing data processing that adversely impacts on an indivdual's right not to be held in slavery or servitude or required to perform forced or compulsory labour.** Schedule 1 of the Human Rights Act (HRA) 1998
☐ Yes – provide details below ☒ No
Click here to enter text
2.5.6 Article 5 – Right to liberty and security **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to liberty and security?** Schedule 1 of the Human Rights Act (HRA) 1998
☐ Yes – provide details below ☒ No
Click here to enter text
2.5.7 Article 6 – Right to a fair trial **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to a fair trial?** Schedule 1 of the Human Rights Act (HRA) 1998 ☐ Yes – provide details below ☒ No

OFFICIAL

Click here to enter text

2.5.8 Article 7 – Right to no punishment without law
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right not to be held guilty of a criminal offence which did not constitute a criminal offence at the time was committed? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.9 Article 8 – Right to respect for private and family life
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to respect for his private and family life, his home and his correspondence? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.10 Article 9 – Right to freedom of thought, conscience and religion
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of thought, conscience and religion?
Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.11 Article 10 – Right to freedom of expression
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of expression? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.12 Article 11 – Right to freedom of assembly and association
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of peaceful assembly and to freedom of association with others? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

OFFICIAL

☒ No

Click here to enter text

2.5.13 Article 12 – Right to marry
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to marry and found a family? [Schedule 1 of the Human Rights Act (HRA) 1998)]

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.14 Article 14 – Right to freedom of discrimination
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of discrimination on any grounds? [Schedule 1 of the Human Rights Act (HRA) 1998)]

☐ Yes – provide details below

☒ No

Click here to enter text

Consultation process with relevant stakeholders

2.6.1 Do you intend to consult others either internally (e.g. business areas, staff associations, TUs etc. other information experts) or externally on the proposed processing?

☐ Yes

☒ No – If you do not intend to consult anyone, you must **justify** why consultation is not appropriate.

Consultation already conducted in 2019 for initial DPIA.

2.6.2 Who do you propose to consult on the proposed processing? List both internal and external organisations/individuals.

N/A

2.6.3 When do you propose to consult with the above organisations/individuals?

OFFICIAL

N/A.
2.6.4 How do you intend to consult with the above organisations/individuals?
N/A

OFFICIAL

Part 2 Section 7 – Assessment and mitigation of risks posed by the proposed processing to the rights and freedoms of data subjects (Refer to Guidance Note 3 of the Part 2 Guidance Notes)

Risk(s) identified to the rights and freedoms of the data subject	**Probability and Impact Score and Risk Level**	**Mitigations**	**Probability and Impact Score and Risk Level after mitigations**	**Result:** The risk is: • Eliminated (E) • Reduced and Acceptable (R/A) • High/Very High and Acceptable (H/A)* • High/Very High and Not Acceptable (H/NA)*	**Evaluation:** Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
RPAS being operated within public area near to persons who perceive an intrusion of privacy by the presence of the RPAS.	Likelihood - 4 Impact - 3 12	RPAS only being used for a genuine policing purpose. RPAS pilots will receive training to include the potential effects of RPAS operations in public areas. RPAS pilots will be overt, uniformed police officers. Officers will ensure open and transparent communication with the public at all times regarding use of RPAS.	Likelihood - 4 Impact - 2 8	R/A	
Access of data by unauthorised persons within Police Scotland.	Likelihood - 1 Impact - 3	All imagery captured via the RPAS SD card is removed and either	Likelihood - 1 Impact - 1	R/A	

OFFICIAL

Imagery captured by RPAS and then viewed by unauthorised staff.	3	transferred to CD for a reporting officer/ enquiry officer/ SIO as a production for criminal proceedings. The CD will be the responsibility of that person and lodged as a production.	1		
Collateral intrusion during imagery capture utilising RPAS. Persons not connected with the policing incident visually recorded by RPAS.	Likelihood – 4 Impact – 3 12	RPAS only being used for a genuine policing purpose. RPAS pilots given guidance on collateral intrusion and how to minimise this effect where possible. Recording of imagery will not be a default setting and the record function activated when required. Data storage and retention policy will be adhered to. Non-evidential data that is not required for any policing purpose will be deleted after 28 days. Evidential data which includes the collateral intrusion by capturing images of persons will be stored securely as evidence and not made available to the	Likelihood – 3 Impact – 2 6	R/A	

OFFICIAL

		public. It will only be accessible by the reporting officer/ enquiry officer/ SIO/ COPFS if required.			
Access of data from the RPAS if obtained by public	Likelihood - 1 Impact - 3 3	Data from RPAS will not be shared with the public unless authorised by Police Scotland and to support an ongoing appeal for information/ investigation. RPAS will be in the possession of police officers at all times whilst in public or stored securely within police premises. If the RPAS requires to be serviced or repaired by an authorised supplier all data will be removed prior to this. The RPAS will be operated within line of sight of the pilots at all times, apart from exceptional threat to life situations. Should the RPAS suffer a malfunction and detach from controlled flight, its final landing site will be marked	Likelihood – 1 Impact – 1 1	E	

OFFICIAL

		and the RPAS recovered by police immediately. If the pilot believes that hostile members of the public will obtain the RPAS before it can be recovered by Police, they can remotely re-format the SD card, deleting all data.			
Use of RPAS without Consent	Likelihood – 1 Impact – 3 3	There will be no requirement to obtain consent from persons within the operating area before deploying the RPAS, as the actions of the police are deemed to be lawful, in “addressing a pressing social need” within a specific policing purpose. Permission will be obtained from Air Traffic Control when flying in certain locations. Should a complaint be made around this at the time of utilising the RPAS, the police officer should advise the person that:	Likelihood - 1 Impact - 1 1	E	

OFFICIAL

		• Non-evidential data that is not required for a policing purpose will be deleted after 28 days. • The data is restricted and is not available to the public, and will only be disclosed to third parties when the circumstances are needed and legitimate. • Recorded data is police information, which can be requested in writing in accordance with the DPA, unless an exemption applies in the circumstances. The RPAS pilot can decide on a case by case basis whether to stop recording, or end the deployment of the RPAS. Though they should be aware that they may need to justify a failure to record an incident just as much as they may need to justify recording it. In all			

OFFICIAL

		cases the use of the RPAS will only be used for a specific policing purpose.			

Once Part 2 of the DPIA is complete it must be returned to IA to ensure the legal requirements are met. Once IA are satisfied that all legal requirements have been met, they will sign it and return it to the project.

*If following mitigations, the risk to the rights and freedoms of individuals remains high, processing cannot commence without the agreement of the Information Commissioner.

OFFICIAL

Approval of DPIA

Information Assurance:

Name: [redacted] (1521525)

Signature: [redacted] (via email)

Date: 16 February 2022

Comments/Observations N/A

Strategic Information Asset Owner (SIAO): Before signing – See Guidance Note 4 in Part 2 of the Guidance Notes

Name:

Signature:

Date:

Comments/Observations