Data Protection Impact Assessment (DPIA) – Stage 2

In this stage of the DPIA process you must provide full details about the lifecycle of the data and the risks associated with the proposal. The information you provide will supplement the information provided in Stage 1.

The aim of this process is to identify and mitigate risks. If any **residual risks** to individuals are **high** then the ICO must be consulted before processing commences.

Section 6 - Impact
Expanding upon the purpose outlined in Section 2.1, please detail the intended effect of the processing on: WMP; the data subjects; and society/the general public Describe the benefits and disadvantages to each of the above.

Effect on WMP

The deployment of drone technology has obvious benefits for West Midlands Police (WMP). It will allow the force to police and respond to incidents in methods not previously available. In responding to incidents the response times can be greatly reduced, capturing vital evidence in a reduced time frame.

In policing public order events the ability to move over the event, identifying potential hotspots of disorder and directing officers on the ground to intercept and disrupt the incidents will be a valuable asset.

Effect on Data Subjects

Due to the manner in which drones capture footage there is an obvious impact on data subjects due to the amount of individuals that would be captured in a single operation for public order events for example. This is unavoidable but is mitigated by virtue that all images captured are reviewed post operation. Only those images deemed to be of an evidential value would ever be retained after an operation and would be focused on individual data subjects only. All other extraneous material would be permanently deleted.

Deployments are concentrated in areas where the privacy expectation is very low, mainly in large densely populated urban conurbations. The majority of image capture would be unidentifiable in relation to personal data due to the sheer volume of images captured.

Effect on Public

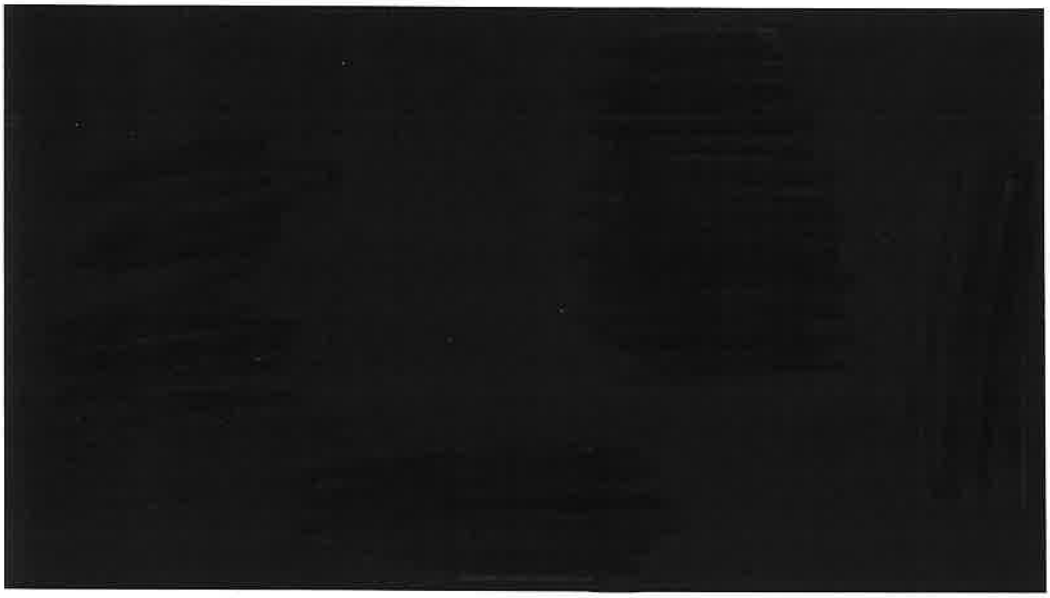
The obvious benefits for society and the general public are that the utilization of drones in policing will allow the force to police, monitor, respond, and capture vital evidence in methods not previously available. The disadvantages are that the wider public may take a view that drones infringe on data subjects right to privacy. Mitigation for this would be that there would be a clear basis under the Law Enforcement Directive (LED) for the capturing and processing of such data.

Section 7 - Information Lifecycle

7.1 Diagrams and Tables

Please insert a diagram or table that demonstrates the flow of data within this proposal. You should reflect the information lifecycle.

[redacted]



7.2 Provide a full description of the information lifecycle

Stage of Processing	Description
Collection Where does the data originate from, who will collect it, how will it be data obtained and how often?	• Data will initially be collected by the drone camera and be collected by the WMP drone pilot. • The frequency of collection is dependent on the number of operations that the drones will have been deployed on.
Storage Describe where and how the data is to be stored	[redacted]Initially the data collected by the drone camera will be stored [redacted] • The pilot operator returns with the drone to a WMP station on the completion of an operation. • The pilot reviews the captured footage and if there is no further requirement for it to be retained then it is immediately permanently deleted. • If it is required further then it is downloaded on to a non-networked WMP laptop. • For evidential purposes the footage will be burned to a

	DVD or copied to an USB stick and transferred on to a networked WMP laptop stored securely in a WMP building.
Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	• Captured footage will only be used if it is of evidential value. • This could be for a number of reasons including:- o Capturing vital evidence following a major incident. o Prevention and detection of crime. o Identification, apprehension, and prosecution of offenders.
Access Describe who has access to the data throughout the life of the processing	• Access will be limited to WMP officers/staff.
Recording Describe the processes for recording the data	• Data is initially recorded to the [redacted]
Processors Describe the use of processors. If a third party is being used then is a contract in place to regulate the relationship? Will the data be processed outside of the UK or the EU?	• There is no third party processor involvement. • No data will be processed outside of the UK.
Sharing With which external organisation(s) is the data shared, what data is shared, and why? Describe any sharing that will occur within WMP Outline any national and international sharing or processing.	• Footage of an evidential value and for use in prosecutions will be shared with Crown Prosecution Service. • Footage could potentially be shared with media outlets to assist in identification of individuals of interest following an incident/event. • The footage will be image capture identifying or to aid in the identification of individuals for a variety of reasons including:- o Prevention and detection of crime o Apprehension and prosecution of offenders o Witnesses or other persons with information about offences
Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate	• All captured footage is immediately reviewed by the WMP officer, operating as the pilot of the drone, on return to a WMP building following the operation involving the drone deployment. • On review footage that is extraneous will be immediately permanently deleted. • Footage of an evidential value will be burned to a DVD/Blu-ray disc or copied to an USB stick and transferred on to a networked WMP laptop. • Footage will be retained for six months pending positive identification of individuals. If at the end of this period no positive identification is made the material will be disposed of. • Footage positively identifying individuals and/or used in

	prosecutions will be retained in line with MoPI guidelines.
Disposal Describe the process for disposal of data, including when and how.	• Footage of an extraneous nature will be permanently deleted following the review after a drone deployment. • DVD/Blu-ray discs following a six month review period will be permanently destroyed by shredding. Material held on USB sticks will be permanently deleted along with any footage stored on the WMP network. • Footage stored in line with MoPI guidelines will be reviewed at the specified date in line with the retention guidelines. If after review it is deemed that it can be disposed it will be conducted as outlined already in the bullet point above.
7.3 Assets Describe the assets that you intend to use.	
Hardware	• See Appendix C
Software	• [redacted] – Drone Management System
Networks	• WMP LAN
Hardcopy/paper	• N/A
Any other relevant assets	• N/A

Section 8 - Consultation	
You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you consider consulting them or their representatives.	
8.1 Do you intend to consult data subjects?	
☐ **Yes** If yes then outline your plan in **Section 8.2** below together with details of consultation with other stakeholders.	
☒ **No** If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 8.2** below.	** Please refer to *Appendix A – Lawful Basis* for a detailed breakdown to justification of not consulting with data subjects.

8.2 Action Log

Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- Data subjects
- The general public
- Union representatives
- Information Security
- DPO
- WMP Legal
- Partner agencies
- NPIRMT
- Data processors
- Information Commissioner's Office (ICO)

Who	When	How	Outcome

Section 9 - Full Risk Assessment

Identify and Assess Risks

In this section you must detail **all** data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. **The assessment criteria outlined in italics in section 9.1 applies to all categories** in Section 9 and 10 i.e. for 'likelihood' you must always assess whether it is 'rare, unlikely, possible, likely or almost certain'.

Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your proposal are considered. If you run out of space then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state **"No risks identified"**.

** Please refer to *Appendix B – Risk Metrics* for a breakdown of the matrices used for calculating and scoring risk.

Examples of **risks to individuals** include: • Discrimination • Identity theft • Financial loss • Reputational damage or embarrassment • Physical harm • Wrongful arrest or prosecution • Loss of confidentiality • Inability to exercise rights	Examples of **corporate risks** include: • Failure to protect the public • Loss of public confidence • Civil litigation • Reputational damage • Regulatory action • Breaching other legal obligations
You should identify **solutions** such as: • Deciding not to collect certain types of data • Reducing the scope of processing • Reducing retention periods • Taking additional technical security measures • Following approved codes of conduct	• Restricting access to data • Training staff to understand the risks • Anonymising or pseudonymising the data • Using different technology • Using an alternative third party processor

9.1 Data Protection Principles

1. Fair and Lawful
- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected and recorded?

2. Purpose Limitation
- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation
- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy
- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Retention
- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all WMP systems if required?
- Is the retention period necessary and proportionate?

6. Security
- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights
- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to the DPO.

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
1	Over processing and capturing of data.	5	3	High	Images are immediately reviewed by the pilot after returning to a WMP station. Only those images of an evidential value are retained further. All other	2	2	Low	Accreditor

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
					images are permanently destroyed.				
2	Loss of data in transit from the drone to ground crew	4	3	**Medium**	[redacted]	1	3	Low	Accreditor
3	Access to data unrestricted and available to non-essential personnel.	2	4	**Medium**	Data is immediately reviewed by the operator crew only following a successful deployment. All extraneous data is permanently deleted. Material of an evidential value is limited to only those personnel required as part of the investigation.	1	4	Low	Accreditor
4	Image data retained for longer than necessary or appropriately.	2	4	**Medium**	All extraneous data is permanently deleted. Footage of an evidential value will initially be retained for six months pending positive identification of individuals. If at the end of this period	1	4	Low	Accreditor

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
					no positive identification is made the material will be securely destroyed/disposed of. Footage positively identifying individuals and/or used in prosecutions will be retained in line with MoPI guidelines.				
5	Data stored insecurely.	2	4	Medium	Data is reviewed on a non-networked laptop. Data that is retained is burned to a DVD/Blu-ray disc or copied to an USB stick and transferred on to a networked WMP laptop in a secure WMP facility. DVD/Blu-ray discs and/or USB's will be stored securely in a WMP facility until their destruction date, see Risk ID 4 for description of retention period,	1	4	Low	Accreditor
6	[redacted]	4	5	Very High	[redacted]	4	3	Medium	Accreditor

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
	[redacted]				[redacted]				
7	There is a risk that the solution does not have auditing built in	3	3	Medium	All system events are captured and system logs are monitored continuously. Logs are managed centrally with the ability to interrogate and manage as relevant in the event of an issue or event. Multiple login failures are recorded. Dip sampling is conducted. Logs are timestamped, with event, status, and error codes with service, command, and application name. The user account associated with an event is recorded.	1	3	Low	Accreditor

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
8	Insufficient access controls in place to limit/restrict users.	5	3	High	Access is limited to only those WMP personnel that are qualified to pilot drones. [redacted] (drone management system) has a clear administration rights structure with an overarching principle user that grants, revokes, restricts access.	1	3	Low	Accreditor
9	Risk that third party personnel will have access to sensitive data.	4	3	Medium	[redacted] personnel are vetted and subject to criminal records checks (DBS). National Police Air Service conducted due diligence on Total AOC with the staff being vetted to sufficient level to have access to the NPAS system. Access is restricted to only [redacted] development, support and operations staff.	2	2	Low	Accreditor

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
10	Third party contractor gaining access to personal data when servicing/repairing individual drones.	4	3	Medium	[redacted]	1	3	Low	Accreditor

9.2 Data Sharing - including the involvement of other Controllers and Processors

- What contracts, MOUs etc are in place or may be required?
- What measures have you taken place to ensure third parties comply with Data Protection laws?
- What risks are involved with sharing data?
- Is sharing necessary and proportionate?
- Is the sharing of data being minimised?

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
1	Lack of formal Information Sharing Agreements (ISA's) or Memorandum Of Understandings (MOU's) for sharing of data. This could lead to the force suffering reputation damage and loss of public confidence along with financial penalties if found	3	4	Medium	Data will be shared with Crown Prosecution Service and viewed in Court in criminal proceedings cases. Sharing agreements are already in place to share such information with the CPS.	1	4	Low	Accreditor

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
	to be in breach of Data Protection legislation.				There is scope in isolated incidents for the footage to be shared with media outlets. This will primarily be for identification purposes of persons of interest in relation to an incident/event or for locating possible witnesses to an incident/event. This is covered under legislation in the DPA 2018 as public task and being in the public interest.				
2	Third party contractor retaining information following the termination of the contract.	4	3	Medium	[redacted]	1	3	Low	Accreditor

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
					[redacted]				
3	Third party contractor has insufficient data protection governance in place to safeguard personal data.	4	3	Medium	[redacted] have been fully risk assessed. Both hold ISO27001 accreditation.	1	3	Low	Accreditor

9.3 International Transfers

- Will data be shared with a third party based outside the EU?
- If you will be making transfers, how will you ensure that appropriate safeguards are put in place?

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
	N/A – there will be no data transfers outside of the EU.	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.	Choose an item.

9.4 Additional Risk Factors
Describe any further risks, ensuring that any risks not already identified are included.

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
	N/A	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.	Choose an item.

Section 10 – Operational Data Risks - Additional Risks Relevant to Operational Data Only

This section is only applicable to proposals involving operational data. **If you are solely processing administrative data then move to Section 11.**

10.1 Data Logging
Where data is processed electronically then logs must be kept for certain actions. This is to enable effective audit of processing systems, data sharing, and to verify ongoing lawfulness of processing.

If the data is processed electronically then will a log be retained of the following actions:	
• **Collection** • **Alteration** • **Consultation** • **Disclosure** • **Combination** • **Erasure**	☒ Yes ☐ No* ☐ Not applicable *If you answered "no" then you must record this as a risk below.

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
	N/A	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.	Choose an item.

10.2 Data Categorisation

When processing data for law enforcement purposes, you must **provide where relevant and as far as possible** a clear distinction between categories of data subject.

Will there be a clear distinction between different categories of personal data suspects, for example subjects who are:	
• **Suspected of having committed, or are about to commit, a criminal offence** • **Convicted of a criminal offence,** • **Victims of a criminal offence,** • **Witnesses to a criminal offence.**	☒ Yes ☐ No* ☐ Not applicable If you answered "no" then you must record this as a risk below.

Risk ID	Risk Description	Likelihood Value	Impact Value	Inherent Risk Rating	Controls	Likelihood Value	Impact Value	Residual Risk Rating	Risk Owner
	N/A	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.	Choose an item.

Section 11 – Outcome and Review			
11.1 Outcome			
Item	**Name**	**Date**	**Notes**
Residual risks approved by:			
DPO advice provided by:			
Summary of DPO advice, including whether the ICO must be consulted:			
11.2 Review			
A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live. Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged.			
Outline: • Who will be responsible for reviewing the processing		• The frequency of review • The date of the next review	

Appendix A – Lawful Basis

As per Article 6 of the GDPR (Part 2 of DPA 2018) it is important that there is a lawful basis for the processing of personal data; this lawful basis for the processing of personal data captured via drone technology is based on the following:

- Public task: The processing of the data can be processed to enable West Midlands Police to carry out their official functions and/or a task in the public interest.

Processing data in this way is necessary in order to enable West Midlands Police officers to more effectively and accurately conduct policing works/operations.

Furthermore, processing of crime data is subject to the Law Enforcement Directive (Part 3 of DPA 2018), and in particular (35) the first data protection principle is satisfied under Section 5 clause (a) as highlighted below:

The first data protection principle

> (2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—
>
> > (b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority.

Processing of special categories of personal data will be conducted under Article 9 of the GDPR (Part 2 of DPA 2018), specifically Article 9.2.g

- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix B – Risk Metrics

Measurement of Likelihood

The likelihood of an event occurring is assessed using the WMP Information Threat Assessment.

Value	Description	Example Detail Description
5	Highly Likely	Is expected to occur in almost all circumstances
4	Very Likely	Will probably occur in most circumstances
3	Likely	Might occur in most circumstances
2	Unlikely	Could occur in some circumstances
1	Zero to Very Low	Occurs only in exceptional circumstances

Measurement of Impact

The impact should an event occur is assessed against a number of factors including cost, reputation and service delivery.

Value	Risk Description	Profile
5	Catastrophic	1) Death 2) Multiple systems are affected 3) Long term loss of service capability 4) Adverse national publicity 5) Litigation almost certain and difficult to defend 6) Financial loss in excess of *£100,000* 7) Breaches of Law punishable by imprisonment
4	Major Impact	1) Extensive, permanent injuries; long term sick 2) Single system at multiple sites affected 3) Medium term loss of service capability 4) Adverse local & national publicity 5) Litigation expected 6) Financial loss between *£50,000 to £100,000* 7) Breaches of law punishable by suspended sentence
3	High Impact	1) Hospitalisation, injuries; medium term sick 2) Multiple systems at single site affected 3) Medium term loss of service capability 4) Local publicity probable; requires careful public relations 5) Litigation possible 6) Financial loss between *£25,000 to £50,000* 7) Breaches of law punishable by fines only
2	Medium Impact	1) Medical treatment required 2) Multiple users affected/Individual system affected 3) Short disruption to service 4) Local publicity is possible 5) Potential for complaint 6) Financial losses between *£5,000 to £25,000* 7) Breaches of regulations/standards

1	Low Impact	1) No injuries beyond first aid level 2) No significant disruption to service 3) Individual user(s) affected/Individual system affected 4) Publicity unlikely 5) Unlikely to cause complaint 6) Financial losses below *£5,000* 7) Breaches of local procedures or standards

Calculation of Risk

The risk value shall be calculated by multiplying the impact and likelihood figures together. This score will then indicate the severity of the risk.

For example:

(Likelihood) **3** x (Impact) **5** = Risk value of **15**

Likelihood						
	5	5 Low	10 Medium	15 High	20 Very High	25 Very High
	4	4 Low	8 Medium	12 Medium	16 High	20 Very High
	3	3 Low	6 Medium	9 Medium	12 Medium	15 High
	2	2 Very Low	4 Low	6 Medium	8 Medium	10 Medium
	1	1 Very Low	2 Very Low	3 Low	4 Low	5 Low
		1	2	3	4	5
		Impact				

Risk Ranking

Risk Ranking	Description
Very High	This is above the organisation's defined tolerance level. The consequences of the risk materialising would have a disastrous impact on the organisation's reputation and business continuity. Comprehensive action is required immediately to mitigate the risk.
High	The consequences of this risk materialising would be severe but not disastrous. Some immediate action is required to mitigate the risk, plus the development of a comprehensive action plan.
Medium	The consequences of this risk materialising would have a moderate impact on day-to-day delivery. Some immediate action might be required to address risk impact, plus the development of an action plan. Status of the risk should be monitored regularly.
Low	The consequences of this risk materialising would have a minor impact. No immediate action is required, but an action plan should be actively considered. Status of the risk should be monitored periodically.
Very Low	The organisation accepts this risk/ impact of risk would be insignificant. Status of the risk should be reviewed occasionally.

Appendix C – Hardware

FSU Drone
Inventory March 202