

Greywolf Graphics Limited
Unit 1, First Floor
37 Colville Road
London W3 8BL

GREYWOLF
GRAPHICS

t: 020 7385 7618

e: studio@greywolfgraphics.co.uk
www.greywolfgraphics.co.uk

Privacy statement

Data protection

We have updated our Data Protection Policy to reflect the regulations (GDPR) introduced in May 2018. We use a Cloud-based CRM system called Capsule to store the names and email addresses of clients and people who may be interested in our services. Occasionally we store mobile telephone numbers too.

From time to time we send marketing emails to our contacts. To do this, we compile an email distribution list using the information stored on Capsule and transfer it to MailChimp, an email marketing distribution service. Both Capsule and MailChimp (data processors) are compliant with GDPR.

We never share personal data with any other companies.

We always give people the option to unsubscribe, and if they do, we immediately remove them permanently from our Capsule records. [Click here](#) for full details data protection notice.

Image protection

Greywolf complies with the code of practice for unmanned aerial systems (UAS) produced by the Information Commissioner's Office, In the picture: a data protection code of practice for surveillance cameras and personal information (<https://ico.org.uk>).

Greywolf pilots, photographers and their operators acknowledge and respect every person's right to privacy. We would not accept camera intrusions into our own personal lives.

Greywolf accepts that it may inadvertently capture visual details of a private nature during the completion of its commercial business (we do not capture audio from our aerial cameras). We are careful to minimise the risk of capturing personal information. In accordance with our operating manual, we assess the impact on personal privacy before every assignment.

All of our material is encrypted and stored on a secure internal server that only two senior employees can access.

We inspect imagery post-project and remove anything that will identify an 'un-suspecting' individual, sensitive location or security system, amongst other criteria. If you feel that we may have captured details of a private or sensitive nature, we will arrange for the imagery to be shown to you at our studio and amended or deleted as requested or instructed.

[Click here](#) to see the relevant sections of the ICO's code of practice.

Image privacy code of practice

Below is a section of the Information Commissioner's Office code of practice that covers Greywolf's operations. We confirm that we always assess the impact on privacy and take every action to minimise the risk of inadvertently capturing personal information. If we do, we will remove it. We make our presence known by wearing hi-vis jackets and direct anyone who has concerns about the legitimacy of our work to the ICO website.

The full version of the ICO's code of practice can be found on its website: <https://ico.org.uk>.

"A distinction should be drawn between those individuals who can be considered as 'hobbyists' and are therefore generally using their 'drones' or cameras for domestic purposes, and those individuals or organisations who use the device for professional or commercial purposes. Where UAS [unmanned aerial systems] are used for non-domestic purposes, operators will need to comply with data protection obligations and it will be good practice for domestic users to be aware of the potential privacy intrusion which the use of UAS can cause to make sure they're used in a responsible manner.

The use of UAS have a high potential for collateral intrusion by recording images of individuals unnecessarily and therefore can be highly privacy intrusive, i.e. the likelihood of recording individuals inadvertently is high, because of the height they can operate at and the unique vantage point they afford. Individuals may not always be directly identifiable from the footage captured by UAS, but can still be identified through the context they are captured in or by using the devices ability to zoom in on a specific person. As such, it is very important that you can provide a strong justification for their use. As with all of the other technologies discussed in this section, performing a robust privacy impact assessment will help you decide if using UAS is the most appropriate method to address the need that you have identified.

As with other technologies discussed, it is important that the recording system on UAS can be switched on and off when appropriate.

This is particularly important given the potential for the cameras to capture large numbers of individuals from a significant height.

Unless you have a strong justification for doing so, and it is necessary and proportionate, recording should not be continuous. This is something which you should look at as part of the privacy impact assessment.

UAS cover the whole system, rather than just the device in the air, so you need to ensure that the whole system is compliant. You should ensure that any data which you have collected is stored securely, for example by using encryption or another appropriate method of restricting access to the information.

You should also ensure that data is retained for the minimum time necessary for its purpose and disposed of appropriately when no longer required.

Example: A business may purchase UAS to monitor inaccessible areas, such as a roof to check for damage.

Its use should be limited to that specific function and recording should not occur when flying over other areas that may capture images of individuals.

You may be able to reduce the risk of collateral intrusion by incorporating privacy by design methods. For example, you may be able to procure a device that has restricted vision so that its focus is only in one place.

Privacy by design can be incorporated into your privacy impact assessment and can form part of your procurement process.

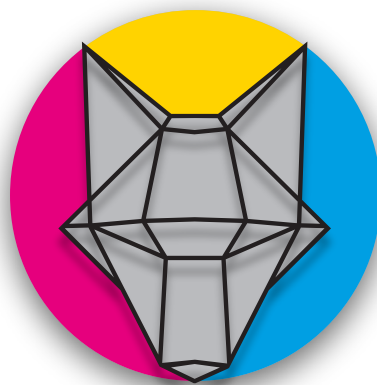
One major issue with the use of UAS is the fact that on many occasions, individuals are unlikely to realise that they are being recorded, or may not know that UAV have a camera attached.

The challenge of providing fair processing information is something that you must address if you decide to purchase UAS.

You will need to come up with innovative ways of providing this information.

For example, this could involve wearing highly visible clothing identifying yourself as the UAS operator, placing signage in the area you are operating UAS explaining its use and having a privacy notice on a website that you can direct people to, or some other form of privacy notice, so they can access further information.

Although these issues are the same as for any aerial vehicle with an attached camera, we have focused here on how UAS can be used as they are a novel device with the potential for a greater impact on privacy."



GREYWOLF
GRAPHICS