



Comhairle Cathrach
& Contae **Luimnigh**

Limerick City
& County Council

Drone Policy

Contents

Document Control	3
1. Introduction/Background	4
2. Purpose of Policy and Procedure	4
3. GDPR Definitions	5
4. Scope	5
5. Purpose of Drone Usage	6
6. Location of Drone Usage	7
7. Data Protection Impact Assessment	7
8. Data Processing Agreements	8
9. Signage and Public Notices	8
10. Insurance	9
11. Designated and Authorised Employees	9
12. Security Arrangements	10
13. Data Subject Access to Drone Recordings	10
14. Third Party Access to Drone Recordings	11
15. Download of Drone Footage	13
16. Users and Access Request Logs	13
17. Retention of Drone Recordings	14
18. Storage and Maintenance	15
19. Purchase of Drones	15
20. Drone Register	15
21. Privacy Statement	15
22. Guidelines/ Codes of Practice	16
23. Data Subjects' Rights	16
24. Complaints to the Data Protection Commission	16
25. Further Information	17
26. Awareness	17
27. Monitoring and Review	17

Document Control

Document Location

Limerick City and County Council Website and Staff Portal

Revision History

Date of this revision: June 2022	Date of next review: June 2023
---	---------------------------------------

Version Number/Revision Number	Revision Date	Summary of Changes
2.0	June 2022	Complete revision of drones policy to include the following sections: Introduction, purpose of drone usage, definitions, signage and public notices, retention, drone register, data subjects' rights, complaints to the data protection commissioner, awareness and monitoring and review. Also expansion and greater detail on existing sections of the policy. Incorporating new European Union Regulation 2019/947.

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
2.0	July 2022	Senior Forum and Mgt Team	Complete revision of existing policy
1.0	Feb. 2019	Mgt Team	Initial Drone Policy approved

Approval

This document requires the following approvals:

Name	Title	Date
	Management Team	08/07/2022
	Senior Forum	04/07/2022
	Management Team	06/12/2019

This policy shall be reviewed on an annual basis by the DPO in consultation with the stakeholders i.e. Environment and Fire and Emergency, and updated as required.

Drone Policy June 2022

1. Introduction/Background

Limerick City and County Council (the Council) is the Authority responsible for Local Government in the City of Limerick and County Limerick in Ireland. It came into operation on the 1st June 2014 after the 2014 Local Elections. It was formed as a result of a merger of Limerick City Council and Limerick County Council under the provisions of the Local Government Reform Act 2014. The corporate headquarters are based at Merchants Quay, Limerick V94 EH90.

Small unmanned aircraft (SUA) i.e. drones are used by the Council for a number of purposes which entail aerial photography and videography. This use may involve the recording of personal data of individuals including their recognisable images. The Council is obliged to protect such data in accordance with provisions contained in the General Data Protection Regulation (GDPR), which came into effect on 25th May 2018, The Law Enforcement Directive (EU 2016/680 (LED) and the Data Protection Acts 1988-2018.

2. Purpose of Policy and Procedure

The Council has developed a number of general policies and procedures to protect personal data. The purpose of this policy and procedures document is to support these documents by outlining specific provisions to assist the Council to fulfil its data protection obligations regarding the operation of drones.

This policy should be read in conjunction with the guidance provided by the Data Protection Commissioner.

Drone operators are required to comply with the flying and operating of drones in accordance with European Union Regulation 2019/947. The Irish Aviation Authority (IAA) supervises and implements those laws in Ireland. Drone operators are also required to comply with the specific operating permission (SOP) issued by the IAA for the use of drones by the Council and any relevant notices and advisory memoranda published by the IAA from time to time. For further information please refer to: <https://www.iaa.ie/>

3. GDPR Definitions

For the purposes of this policy and procedures document, the following definitions apply:

- **Council:** means Limerick City and County Council.
- **Data Controller:** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Data Subject:** is an individual who is the subject of personal data.
- **Personal Data:** any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing:** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Processor:** a natural or legal person, public authority, agency or other body that processes personal data on behalf of the Council.

4. Scope

The scope of this policy and procedures document applies to all:

- The Council use of drones that may include the recording of personal data.
- The Councils' Authorised Officers and third party drone service providers that may be engaged by the Council.

5. Purpose of Drone Usage

5.1. When deciding to use a drone for any particular purpose which involves the recording of personal data, the Council shall seek to ensure that at least one of the conditions outlined in Articles 6 (and where relevant Article 9 of the GDPR or Articles 8 (and where relevant Article 10) of the Law Enforcement Directive EU 2016/680 (LED) and sections 71 (and where relevant section 73) of the Data Protection Act 2018 exists to ensure the lawfulness of the processing of the personal data involved.

5.2. Drones may be used by the Council for the following but not limited to:

- The provision of emergency services and operations, such as those that may be provided by the Fire Service;
- Aerial surveying, photographing and mapping;
- Evidence gathering to assist enforcement activities such as those that may be carried out by the Planning and Environment Sections of the Council for example pursuant to Section 14 of the Waste Management Act 1996. Under that section an Authorised Officer may enter premises or board vehicles and deploy drones at all reasonable times and at any time where an Authorised Officer has reasonable grounds for believing that there may be a risk of environmental pollution arising from the carrying on of an activity at any premises or that such pollution is occurring provided always that before entering any private dwelling an Authorised Officer must give notice or obtain consent from the occupier in accordance with Section 14 or secure a warrant to enter the premises where an Authorised Officer is prevented from entering any premises or has reason to believe that evidence related to a suspected offence under that Act may be present in any premises and that the evidence may be removed therefrom or destroyed;
- Prevention, detection, and investigation of environmental crime;
- Protection of human health and property, search, rescue and recovery services;
- Marketing and promotional reasons.

5.3 Personal data obtained through the use of drones shall be limited and proportionate to the purposes for which it was obtained.

5.4 Drones will not be used by the Council for any purposes other than those outlined in this document.

6. Location of Drone Usage

- 6.1. Drones may be used, in any location where it is considered appropriate, for any of the purposes outlined in this document. Drone operators must follow the process outlined in Section 9 of this policy with regard to Signage and Public Notices.
- 6.2. Appropriate measures will be taken to ensure that drone recordings are limited to the target area and the purpose for which the drone has been deployed.
- 6.3. A drone's functionality should be appropriate for the intended purpose. Drone operators should consider measures to limit the unnecessary recording of personal data that is not required.
- 6.4. All flights within controlled airspace, restricted, prohibited and densely populated areas may only be carried out where the appropriate permissions are in place. Drone operators must ensure that they adhere to the UAS Aeronautical Notices issued by the IAA from time to time and any other process specified by the IAA, where applicable e.g. restrictions on flying a drone within Shannon Airport Controlled Airspace (CTR).

7. Data Protection Impact Assessment

- 7.1. Article 27 of the LED (complimented by Recital 58) and Section 84 of the Data Protection Act 2018 set out the circumstances under which a DPIA must be conducted and the minimum requirements that process must meet to achieve legal compliance. In line with those requirements and DPC guidance relating to the use of drones a Data Protection Impact Assessment (DIPA) must be carried out before any drone operations. A DPIA may also be required for an upgrade to an existing drone model or its capabilities, if in the opinion of the Council, the installation or upgrade is likely to result in a high risk to the rights and freedoms of individuals. The purpose of a DPIA will be to facilitate the identification and implementation of appropriate measures to eliminate or minimise any risks arising out of the processing of personal data by a drone system.
- 7.2. A draft DPIA must be submitted to the Data Protection Officer for review and final DPIA signed off by the relevant Responsible Person in the relevant department.

7.3. DPIA'S should be reviewed every 3 years (as per DPC Guidance).

7.4. For each individual drone flight, a separate risk assessment must be carried out and logged appropriately.

8. Data Processing Agreements

8.1. Service providers that have access to personal data recorded by drones are considered to be a Data Processor and as such are required to enter into a formal Data Processing Agreement with the Council to ensure that they, in addition to the Council, discharge their obligations under data protection legislation.

9. Signage and Public Notices

9.1. Drone operators will be easily identifiable as they will be wearing high visibility vests stating that they are drone operators;

9.2. Signage will be placed in the vicinity of the drone operator or in appropriate circumstances simply around the drone operator when drone activity is being carried out to advise the public of the following:

9.2.1. Name of Data Controller i.e. Limerick City and County Council.

9.2.2. Drone activity is taking place.

9.2.3. Purpose for which the drone activity is being carried out.

9.2.4. Contact details for enquiries by members of the public.

9.3. Following the carrying out of any drone activity, consideration should be given to placing a notice on the Council's social media channels and website to advise the public of the Council's use of drones. The following details shall be provided at a minimum on any such notices:

9.3.1. Statement that the Council has carried out drone activity.

9.3.2. Dates, times and locations that drone activity took place.

9.3.3. Purpose for which the drone activity was carried out.

9.3.4. Contact details for enquiries by members of the public.

9.4. For any reason that the above cannot be complied with, the reasons and rationale will be documented in the site specific risk assessment, e.g. risk of threat or assault to drone

operator and observer.

10. Insurance

10.1. Use of the Drone is covered under the Council's insurance (Remotely Piloted Aircraft Extension under the Public Liability Policy). It is a condition precedent to the Insurer's liability under this Extension that such remotely piloted aircraft system shall;

- be restricted to a maximum weight of 20 kilograms (excluding fuel but including articles or equipment installed or attached).
- be restricted to activities related to educational, research, risk assessment, photographic evidence and surveying work.
- exclude the operation of remotely piloted aircraft systems for military purposes.
- comply with all applicable legislation and Irish Aviation Authority requirements.
- have comparable public liability insurance cover in place as well as the applicable licence and permits when the council are procuring a third party drone operator.

11. Designated and Authorised Employees

11.1. The CEO as the Accountable Manager will delegate responsibility for the overall operation of each drone system to the UAS Responsible Person, such as the relevant Director of Services or appropriately competent person. This responsibility will include ensuring that the system is being operated in a manner that is consistent with this policy and procedures document, Data Protection legislation and the European Union Regulation 2019/947.

11.2. Only staff that have been nominated as Authorised Officers for each drone system may have access to the system and its recordings. Authorised Employees should include the following:

- Designated Employees who may access the drone system(s) for which they have been assigned responsibility;
- Drone Operators that are licenced by the IAA;
- IT Department Staff who may access all the Council drone systems for the purposes of carrying out maintenance and upgrade works.
- Data Protection Officer who may access all the Council drone systems and their recordings.

11.3. The relevant Director of Services for each drone system shall ensure that

Authorised Employees are appropriately trained before operating takes place.

12. Security Arrangements

- 12.1. Access to drones and their recordings will be subject to appropriate security arrangements and controls to safeguard against any unauthorised access or disclosure including by Authorised Officers and any authorised third party drone service providers that may be engaged by the Council.
- 12.2. The data storage facility on a drone shall be erased after each use unless the original storage media is required to be retained for legal proceedings. The drone operator will review the footage to determine if evidence needs to be retained. If in doubt, consult with the Responsible Person.
- 12.3. Recordings may only be extracted and stored on the SharePoint storage platform provided the copies of the drone recordings are:
 - Required to be retained in accordance with provisions outlined in this policy and procedures document.
 - Stored in a secure location with access restricted in accordance with provisions outlined in this policy and procedures document.
- 12.4. Where imagery from drones is required to be transferred to a third party, for example, An Garda Síochána in the circumstances set out in this policy, that transfer shall take place via a secure encrypted Sharefile system. In limited circumstances where broadband may be an issue, an encrypted USB (Bitlocker) device or encrypted hard drive (Bitlocker) will be used to transfer the footage. The USB drive will be hand delivered or collected by the third party and accompanied by chain of custody documentation to ensure the integrity of the data for evidential purposes.

13. Data Subject Access to Drone Recordings

- 13.1. Data protection legislation provides data subjects with a right to access their personal data. This includes their recognisable images and other personal data captured by drone recordings. Access requests should be submitted in writing in physical or electronic format e.g. by letter or e-mail to the Data Protection Officer and will be processed in accordance with provisions

contained in the Council's Subject Access Request Policy and Procedures.

13.2. It will generally not suffice for a data subject to make a general access request for a copy of drone recordings. It will usually be necessary that data subjects specify that they are seeking to access a copy of drone recordings that have captured their recognisable images and/or other personal data between specified dates, at certain times and at a named location. The provision of access to a data subject to drone recordings of his/her recognisable images and/or other personal data will normally involve providing a copy of the recording in video format using a secure methodology. In circumstances where the supply of a copy of the recording to the data subject is not possible or would involve unreasonable effort or cost, stills may be provided as an alternative to video footage. Where stills are provided, the Council will aim to supply a still for every second of the recording in which the data subject's recognisable images and/or other personal data appears.

13.3. Where recognisable images and/or other personal data of parties other than the data subject appear on the drone recordings these will be pixelated or otherwise redacted on any copies or stills provided to the data subject. Alternatively, unedited copies of the drone recordings may be released provided consent is obtained from those other parties whose recognisable images and/or other personal data appear on the drone recordings.

13.4. If the drone recording does not clearly identify recognisable images and/or other personal data relating to the data subject then the recording will not be considered as personal data and will not be released by the Council.

13.5. If the drone recording no longer exists on the date that the Council receives an access request it will not be possible to provide access to a data subject. Drone recordings are usually deleted in accordance with provisions contained in this policy.

14. Third Party Access to Drone Recordings

Access to drone recordings may be provided, using a secure methodology, to the following:

- An Garda Síochána.
- Legal Advisors.

- Other third parties, such as statutory prosecution agencies and local government agencies for example, with WERLA for prosecutions, EPA and other local authorities under section 41(b) of the data protection act 2018 .

14.1. Access by An Garda Síochána

14.1.1. The provision of personal data, including drone recordings, to An Garda Síochána for the purposes of investigating and/or prosecuting a criminal offence is permitted under provisions contained in the Data Protection Act 2018.

14.1.2. Requests from An Garda Síochána for copies of drone recordings are required to be submitted in writing on An Garda Síochána headed paper and signed by an appropriate ranking member of An Garda Síochána. The request should specify the details of the drone recordings required and affirm that access to such recordings is necessary for the investigation and/or prosecution of a criminal offence.

14.1.3. In order to expedite a request in urgent situations, a verbal request from An Garda Síochána for copies of drone recordings will suffice. However, such a verbal request must be followed up with a formal written request from An Garda Síochána.

14.2. Access by Legal Advisors

Access to drone recordings will be provided, where required and in accordance with data protection legislation, to the Council's legal advisors for the purposes of carrying out enforcement action, for claims management purposes and in any other circumstance that is considered necessary and appropriate.

14.3. Access by Other Third Parties

Access by third parties other than An Garda Síochána, WERLA and the Council's legal advisors to drone recordings will only be provided in circumstances that are permitted by Data Protection legislation such as local authorities under Section 41(b) of the Data Protection Act 2018.

15. Download of Drone Footage

- 15.1. Footage downloaded from the drone shall be securely stored with restricted viewing access.
- 15.2. Any personal data not required for prosecution purposes shall be deleted as soon as practicable.
- 15.3. Any personal data required for prosecution purposes shall be retained only for as long as necessary and deleted when no longer required.
- 15.4. All other photographic or video data shall be retained only as long as it is required for comparison /monitoring/legal purposes.

16. Users and Access Request Logs

16.1. Users Log

The Administrator that has responsibility for each drone system shall ensure that a Users Log is being maintained by drone operators. This log shall include details of:

- Name of drone operator.
- Details of drone used.
- Dates and times of use.
- Purpose of use.
- Location of use.

16.2. Incident Log

The Designated Employee that has responsibility for each drone system shall ensure that an Incident Log e.g. abandonment of a flight or grounding of flight or unable to fly is being maintained by drone operators. This log shall include details of:

- Name of drone operator.
- Details of drone used.
- Dates and times of use.
- Details of incident
- Details of third party involvement

- Action taken

16.3. Data Subject Access Requests Log

The Data Protection Officer shall record all details of all Access Requests made by Data Subjects and the outcome of such requests on a separate log that is maintained for this purpose.

16.4. Third Party Access Requests Log

A Third Party Access Requests Access Log shall be maintained by the Designated Employee that has responsibility for each drone system. This log shall maintain a record of all requests made by the following third parties to view/obtain copies of drone recordings and the outcome of such requests:

- An Garda Síochána.
- Legal advisors.
- Other third parties.

17. Retention of Drone Recordings

- 17.1. Personal Data recorded by drones should be kept for no longer than is considered necessary.
- 17.2. In the majority of cases, the Council will not retain personal data recorded by drones beyond a maximum of 28 days.
- 17.3. Personal data recorded by drones may however be retained by the Council beyond a maximum of 28 days in a limited number of circumstances. These include situations where the retention of the personal data is necessary for operational purposes e.g. for surveying activities, project based work and for investigative, evidential and legal purposes. Staff should contact the Data Protection Officer for advice if they are unsure of retention obligations.

18.Storage and Maintenance

- 18.1 The physical storage, maintenance, and flight-readiness preparation of drones operated by an appointed Responsible Person within each department.
- 18.2 The drone shall be stored securely when not in use, but also to prevent unauthorised use.

19. Purchase of Drones

- 19.1 Under GDPR, the Council must maintain a central register of all data processing activities; as drones have the potential to record and capture personal data (e.g. images of people /car registration numbers) they must be included on this register.
- 19.2 Any drone purchased prior to the date of this policy must be notified to the Data Protection Officer immediately (if not already done).
- 19.3 Any future proposals regarding purchase of additional drones must be notified in advance to the Data Protection Officer.

20.Drone Register

A drone register shall be maintained by the Data Protection Officer. This register shall contain, at a minimum, the following information:

- Location of drone systems.
- Purpose of each drone system.
- Legal basis for the processing of personal data.
- Details of Designated and Authorised Employees.
- Drone system service provider details.
- Access/security controls.
- Retention period for drone recordings.

21.Privacy Statement

Details of personal data being recorded by drone systems that are used by various Departments/Business Units of the Council and information regarding the use of

such data including any sharing of such data with third parties are outlined in a Privacy Statement. A copy of this Privacy Statement may be accessed at <https://www.limerick.ie/council/services/your-council/data-protection/data-protection-privacy-statement-limerick-city-and>

22.Guidelines/ Codes of Practice

The Council shall adhere to all relevant Guidelines/Codes of Practice pertaining to the use of drones including any guidelines and codes of practice issued under relevant legislation, by the Data Protection Commission, by the Irish Aviation Authority, and/or by other relevant statutory bodies.

23.Data Subjects' Rights

Where drone recordings contain images of you, these images are your personal data and you have the following statutory rights in relation to this data which can be exercised at any time:

- a) Right to information.
- b) Right to complain to supervisory authority.
- c) Right of access.
- d) Right to rectification or erasure.
- e) Right to be forgotten.
- f) Right to restrict processing.
- g) Right to data portability; and
- h) Right to object and automated decision making/profiling.

For further information, please see our Data Protection Policy available at <https://www.limerick.ie/council/services/your-council/data-protection/data-protection-privacy-statement-limerick-city-and> or alternatively contact our Data Protection Officer at the contact details listed below.

24.Complaints to the Data Protection Commission

24.1. Data subjects may make a complaint to the Data Protection Commissioner in the following circumstances:

- If they experience a delay outside of the prescribed timeframe for making a decision on an access request or if they are dissatisfied with a

decision by the Council on their access request.

- If they consider that the Council's processing of their personal data is contrary to their data protection rights.

24.1.1. Contact details for the Data Protection Commission are as follows:

Phone Number: 0761 104 800

E-mail: info@dataprotection.ie

Website: www.dataprotection.ie

Postal Address: Data Protection Commission, Canal
House, Station Road, Portarlinton, Co. Laois, R32
AP23

25. Further Information

Further information on the operation of this policy and procedures document is available from the Data Protection Officer, Limerick City and County Council.

Contact details for the Data Protection Officer are as follows:

Phone Number: 061 556000

E-mail: dataprotectionofficer@limerick.ie

Website: www.limerickcouncil.ie

Postal Address: Limerick City and County Council, Merchant's Quay, Limerick V94 EH90.

26. Awareness

26.1. The Council shall implement appropriate measures to make its employees and other relevant parties aware of the content of this policy and procedures document.

26.2. All persons involved in the planning, placement and operation of the Council drones should familiarise themselves with the content of this policy and procedures document.

27. Monitoring and Review

Provisions contained in this policy and procedures document shall be subject to ongoing monitoring and review.