**CRAOL-Community Radio Forum of Ireland Society Ltd Data Protection Policy**

**1 Introduction**

This Policy sets out the obligations of CRAOL Community Radio Forum of Ireland Society Ltd **hereafter referred to as CRAOL,** in regard to Data Protection. It outlines the responsibilities of Craol in maintaining and ensuring the rights of all staff both employed and voluntary, Craol learners, trainers, assessors, network members, associate members and all other interested parties in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

GDPR defines “personal data” as any information relating to an identified or identifiable natural person (“a data subject”). An identifiable 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 physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

**2 Scope**

This policy applies to all personal data created or received by Craol in all formats. It sets out Craol’s obligations regarding collection, processing, transfer, storage and disposal of personal data for all Craol network station staff affiliated with Craol, learners and other interested parties. The procedures and principles set out herein must always be followed by the organisation, (both employed and voluntary) and by external agents, contractors, or other parties working on behalf of the organisation.

**3. Date of Issue**

This policy was implemented on 25th May 2018 and was last reviewed on September 2022. No part of this Policy shall have retroactive effect and shall apply only to matters occurring on or after this date. It will be reviewed annually or subject to changes in GDPR.

**4 Data Protection Principles**

As a Data Controller, Craol is responsible for, and must be able to demonstrate compliance with Data Protection Law. This means complying with and demonstrating that the key principles of Data Protection are met according to The ‘General Data Protection Regulation’ (GDPR). GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

**4.1** Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

**4.2** Collected for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This includes processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

**4.3** Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

**4.4** Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

**4.5** Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data is processed.

**4.6** Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**The Rights of Data Subjects**

GDPR sets out the following rights applicable to data subjects.

**5.1** The right to be informed. (Section 13.)

**5.2** The Right of access. (Section 14).

**5.3** The Right to rectification. (Section 15).

**5.4** The right to erasure (also known as the ‘right to be forgotten’). (Section 16).

**5.5** The right to restrict processing. (Section 17).

**5.6** The right to data portability. (Section 18).

**5.7** The right to object. (Section 19).

**6 Lawful, Fair, and Transparent Data Processing**

**6.1** Craol seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Craol follows the GDPR guidelines which state that the processing of personal data is lawful if least one of the following applies:

 6.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes.

 6.1.2 The processing is necessary for the performance of a contract to which the data subject is a party.

 6.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject.

6.1.4 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child or vulnerable adult.

6.1.5 The processing is necessary for archiving purposes and in the public interest, scientific or historical research purposes, or statistic purposes in accordance with Article 89 (1) of the GDPR.

**6.2** For the processing of ‘special category information’ (sensitive personal data) for example, data concerning the data subject’s race, ethnicity, politics, religion, genetics, biometrics (if used for ID purposes), health or sexual orientation GDPR guidelines which state that at least one of the following conditions must be met:

 6.2.1The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

 6.2.2 Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

 6.2.3 Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

 6.2.4The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.

**7 Specified, Explicit, and Legitimate Purposes**

**7.1** Craol collects and processes the personal data collected directly from data subjects and personal data obtained from third parties.

**7.2** Craol will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed.

**7.3** Data subjects are always kept informed of the purpose or purposes for which Craol uses their personal data.

1. **Accuracy of Data and Keeping Data Up to Date**

**8.1** Craol will ensure that all personal data collected, processed, and held is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Section 15 of this policy.

1. **Data Retention**

**9.1** Craol will not keep personal data for any longer than is necessary for the purpose/s for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

**9.3** For full details of Craol’s approach to data retention, including retention periods for specific personal data types held by the organisation, please refer to the Craol Data Retention Policy.

**10. Secure Processing**

Craol ensures that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

**11. Accountability and Record-Keeping**

**11.1** The organisation’s Project Coordinator is responsible for overseeing the implementation of this Policy, monitoring compliance with this Policy and any other Craol Data Protection-related policies, and with keeping up to date with GDPR and other applicable data protection legislation.

**13. Keeping Data Subjects Informed**

**13.1** Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection.

**13.2** Where personal data is obtained from a third party, the relevant data subjects will be informed of the purpose of its collection, and how Craol processes this information.

**13.3** Details of the data subject’s rights in relation to third party information are set out in the Craol Privacy Policy.

**14. Data Subject Access**

**14.1** Data subjects may make subject access requests (“SARs”) at any time to find out more about the personal data which the organisation holds about them, what it is doing with that personal data, and why. This can be done by writing to Craol and marking the correspondence **Subject Access Request**.

**14.2** Responses to SARs will be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

**14.3** Craol will not charge a fee for the handling of SARs but reserves the right to charge reasonable fees for additional copies of information that have already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

**15. Rectification of Personal Data**

**15.1** Data subjects have the right to require the organisation to rectify any of their personal data that is inaccurate or incomplete. The organisation will undertake to rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Craol of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

**15.2** In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

**16. Erasure of Personal Data**

**16.1** Data subjects have the right to request that Craol erases the personal data it holds about them in the following circumstances:

 16.1.1 It is no longer necessary for the organisation to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.

 16.1.2The data subject wishes to withdraw their consent to the organisation holding and processing their personal data.

16.1.3The data subject objects to Craol holding and processing their personal data (and there is no overriding legitimate interest to allow the organisation to continue doing so) .

 16.1.4The personal data has been processed unlawfully.

 16.1.5 The personal data needs to be erased in order for Craol to comply with a legal obligation.

**17. Restriction of Personal Data Processing**

**17.1** Data subjects may request that Craol ceases processing the personal data it holds about them. If a data subject makes such a request, the organisation shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

**17.2** In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

**18. Objections to Personal Data Processing**

**18.1** Data subjects have the right to object to Craol processing their personal data based on legitimate interests or direct marketing (including profiling).

**18.2** Where a data subject objects to Craol processing their personal data based on its legitimate interests, the organisation shall cease such processing immediately, unless it can be demonstrated there are legitimate grounds for such processing which override the data subject’s interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

**19. Data Security - Transferring Personal Data and Communications**

Craol commits to ensuring the following measures are taken with respect to all communications and other transfers involving personal data:

**19.1** All emails containing personal data must be marked “confidential”.

**19.2** Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

**20. Data Security - Storage**

Craol commits to ensuring the following measures are taken with respect to the storage of personal data:

**20.1** All electronic copies of personal data should be stored on encrypted drives and devices securely using passwords and data encryption where appropriate.

**20.2** All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.

**20.3** No personal data should be transferred to any device personally belonging to an employee/volunteer and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Craol where the party in question has agreed to comply fully with the letter and spirit of this Data Protection Policy and of GDPR regulations (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

**21. Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to Craol’s Data Retention Policy.

**22. Data Security - Use of Personal Data**

Craol commits to ensuring the following measures are taken with respect to the use of personal data:

**22.1** No personal data may be shared with an employee/volunteer, external sub-contractor, or other party working on behalf of Craol without consent.

**22.2** Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised person including but not limited to learners, trainers, internal/external assessors, employees/volunteers, external sub-contractors, whether paid or voluntary, or any other parties at any time.

**23. Data Security - IT Security**

Craol will ensure that the following measures are taken with respect to I.T. and information security:

**23.1** All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used Craol is designed to require such passwords.

**23.2** Under no circumstances should any passwords be written down or shared between any staff of Craol, whether paid or voluntary, external assessors, trainers, learners, or any other parties working on behalf of the organisation, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

**23.3** All software (including, but not limited to, applications and operating systems) shall be kept up to date.

**24. Organisational Measures**

Craol commits to ensuring the following measures are taken with respect to collection, holding and processing of personal data. All Craol employees, whether paid or voluntary, sub-contractors and external parties working on behalf of Craol handling personal data will be:

* Appropriately trained and bound to do so in accordance with the principles of the GDPR and this Policy.
* Be made fully aware of both their individual responsibilities and the organisation’s responsibilities under GDPR and under this Data Protection Policy and shall be provided with a copy of this Policy.
* Only have access to personal data if they need to do so in order to carry out their assigned duties correctly.
* Be required and encouraged to exercise care, caution, and discretion when discussing work related matters that relate to personal data, whether in the workplace or otherwise.

**24.1** All personal data held by Craol will be reviewed periodically as set out in the organisation’s Data Retention Policy and methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

**24.2** Where any external contractor or other party working on behalf of Craol handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Craol against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

**25. Data Breach Notification**

**25.1** All personal data breaches must be reported immediately to the Craol’s Data Protection contact person as soon as possible.

**25.2** If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection contact person must ensure that the Data Protection Commission is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

**25.3** Data breach notifications shall include the following information:

 26.4.1 The categories and approximate number of data subjects concerned.

 26.4.2 The categories and approximate number of personal data records concerned.

 26.4.3The name and contact details of Craol’s Data Protection contact person (or other contact point where more information can be obtained).

 26.4.4 The likely consequences of the breach.

 26.4.5 Details of the measures taken, or proposed to be taken, by the organisation to

address the breach including, where appropriate, measures to mitigate its possible

adverse effects.