iacat
Irish Association of
Creative Arts Therapists

iacat GDPR Policy

May 2022

Approved by council 2022

Data Protection Policy

1 Introduction

IACAT are committed to protecting the rights and privacy of individuals in accordance with applicable data protection legislation, amended from time to time, including the Data Protection Acts 1988-2018, the ePrivacy Directive 2002/58 enacted in Ireland by S.I. No. 336 of 2011 and the General Data Protection Regulation EU 2016/679 ("GDPR"). "Applicable Data Protection Legislation".

2 Information on Processing

IACAT collects, uses and keeps (process) Personal Data relating to its registered members, student members, suppliers and volunteers (Data Subjects). The categories of Personal Data processed are:

> Names, email addresses, home addresses, contact numbers, emergency contact details.

The Personal Data is processed for the following purposes:

> For recording on members database, for contacting in relation to membership and volunteer work and for the arrangement of work by and payment of suppliers where applicable.

The Personal Data is processed by the following categories of recipients:

> Officers and Administrators of IACAT.

The legal basis for processing the personal data is for the purposes of fulfilling contracts that the Data Subjects enter with IACAT.

The Personal Data is kept for no longer than is necessary for the purposes for which it is collected.

IACAT are classified as a Data Controller **under the** Applicable Data Protection Legislation**.**

3 Purpose and Scope

This policy is a statement of IACAT's commitment to protect the fundamental rights and freedoms of individuals in accordance with Applicable Data Protection Legislation. Data protection obligations outlined relate to Personal Data of IACAT's Data Subjects.

This Policy applies to all who are authorised to process data on behalf of IACAT, including its officers and administrator. They are collectively referred to as "Users" from this point.

4 Data Protection Principles

As a Data Controller, IACAT must comply with the data protection principles which are set out in the Applicable Data Protection Legislation. The Data Protection Responsible Person

in IACAT maintains a Data Map of Personal Data held within the organisation to demonstrate its compliance with the data protection principles.
IACAT will administer its responsibilities under the legislation in accordance with these stated principles as follows:

- **Lawfulness, Fairness and Transparency**
  IACAT will obtain and process Personal Data fairly in accordance with the Applicable Data Protection Legislation. **This means that** IACAT **must ensure that the Data Subject has been provided with details relating to the uses and disclosures that will be made of their data and is informed of their access and amendment rights (see section 6 below). Compliance with this obligation is achieved through the sharing of this policy with its users.**

  IACAT **must process Personal Data and Special Category Data in accordance with its legal obligations. This includes an obligation under the** Applicable Data Protection Legislation **to legitimise the processing of Personal Data. In respect of Personal Data, processing must be legitimised on the basis that processing is necessary for certain purposes specified in the** Applicable Data Protection Legislation **including:**

  - **the legitimate interests of** IACAT **or third parties to whom the data is disclosed except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data;**
  - **the performance of a contract to which the Data Subject is party;**
  - **the performance of a statutory function;**
  - **the performance of a legal obligation (provided it does not arise under contract); or**
  - **the prevention of injury or damage to the health of the Data Subject or another person, damage to property or to otherwise protect a person's vital interests.**
  - **Or the data subject has given demonstrable, clear, specific and informed consent to the processing of their Personal Data.**

  Additional criteria must be satisfied to legitimise the processing of Special Category Data with the result that explicit consent to processing is usually required. There are a number of limited alternatives to explicit consent set out in the Applicable Data Protection Legislation **including scenarios where the processing is necessary for:**

  - **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 in so far as it is authorises by law, providing for appropriate safeguards for the fundamental rights and the interests of the data subject; and**

- **protecting the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent;**
- protecting the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- **processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the customers or others of or former customers or other contacts of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data is not disclosed outside that body without the consent of the data subjects;**
- processing Personal Data which are manifestly made public by the data subject;
- **the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;**
- **for reasons of substantial public interest, on a legal basis 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;**

Where consent is being relied on as the legal basis for processing, Data Subjects must be informed that they may withdraw their consent at any time.

• **Purpose Limitation**

IACAT will only collect Personal Data for specified, explicit and legitimate purposes and not further process it in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

• **Data Minimisation**

IACAT will only **process Personal Data that is** adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

• **Accuracy**

IACAT will ensure that the Personal Data it processes is accurate and, where necessary, kept up to date. **Every reasonable step will 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

- **Storage Limitation**

IACAT will ensure that Personal Data is kept in a form which permits identification of data subjects, for no longer than is necessary for the purposes for which the personal data are processed. Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest,

scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by Applicable Data Protection Legislation in order to safeguard the rights and freedoms of the data subject

• **Integrity and Confidentiality**

IACAT will ensure that it and any third parties whom it engages to process Personal Data on its behalf will process the Personal Data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Note: IACAT will always be regarded as the Data Controller **in relation to Personal Data of which it controls the contents and use.** All third parties and external parties acting as **Data Processors** must comply with Principle vi (i.e. integrity and confidentiality) **and process the data solely in accordance with the written instructions of** IACAT. **As the Data Controller**, IACAT is obliged to **ensure that a written contract (the "Data Processor Agreement") is put in place with third party processors and the terms of said Data Processor Agreement comply with requirements of Applicable Data Protection Legislation.**

5 Accountability

Roles/Responsibilities

As the Data Controller, IACAT has overall responsibility and must be accountable for ensuring that it complies with its obligations under the **Applicable Data Protection Legislation**. However, all Users working on behalf of IACAT who, as part of their responsibilities, process Personal Data about **identifiable individuals**, either in an automated **or manual form**, must comply with this policy. IACAT will provide support, assistance, advice, and training to appropriate individuals who are handling such data in order to ensure that they are in a position to comply with this policy.

Under **Applicable Data Protection Legislation,** IACAT **must be able to demonstrate its compliance with such Applicable Data Protection Legislation, through its behaviour, its written procedures and its record keeping of processing activities.**

It is the responsibility of IACAT Data Protection Responsible Person to formulate such written procedures and records of processing activities, and to provide direction in matters concerning data protection.

6 Rights of Data Subjects

Data Subjects have the following rights under Applicable Data Protection Legislation:

- a right of access to their Personal Data;
- a right to seek rectification of their Personal Data;
- a right to request erasure of their Personal Data;
- a right to request the restriction of processing in certain circumstances, described fully in the Applicable Data Protection Legislation;
- a right to object to processing of any Personal Data that is being kept about them **by** IACAT on computer systems or in manual files;
- a right to data portability which will allow the Personal Data be transferred from IACAT to another Data Controller, in a structured, commonly used and machine readable format; and
- a right not to be the subject of a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject, or significantly affects the data subject.

These rights are subject to certain exemptions and conditions which are set out in the Applicable Data Protection Legislation.

Any person who wishes to exercise these rights should make the request in writing to the Data Protection Responsible Person.

All Data Subject requests will be responded to in accordance with the Applicable Data Protection Legislation and the responses will be managed by the Data Protection Responsible Person.

Any queries, written or verbal, received by any officer, administrator or member, from An Garda Síochána, the Revenue Commissioners, Local Authorities or any other State Agency seeking access to any Personal Data held by IACAT should be referred **immediately** to the Data Protection Responsible Person.

7 Marketing

The Applicable Data Protection Legislation confers rights on data subjects in respect of the use of their data for marketing purposes. Rights vary according to the means of communication used**,** whether the party is an individual or a corporate entity **and whether or not the party is in a contractual relationship with** IACAT**, or whether** IACAT **has a legitimate purpose for** use of their data for marketing purposes, or whether the party **has a legitimate expectation of** IACAT use of their data for marketing purposes.

8 Transfer of Data Outside of the European Economic Area (EEA)

All data transfers that include Personal Data must be approved by the Data Protection Responsible Person.

There is a general prohibition on the transfer of personal **to countries** outside of the EEA (EU member states plus Switzerland, Norway, Iceland and Liechtenstein) which the European Commission does not regard as conferring an adequate level of data protection.

Where Personal Data must be transferred outside the EEA, one of the following conditions must be met by IACAT:

- consented to by the data subject; or
- required or authorised under an enactment, convention or other instrument imposing an international obligation on this State; or
- necessary for the performance of a contract between the data controller and the data subject; or
- necessary for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller; or
- necessary for the conclusion of a contract between the data controller and a third party, that is entered into at the request of the data subject and is in the interests of the data subject, or for the performance of such a contract; or
- necessary for the purpose of obtaining legal advice; or
- necessary to urgently prevent injury or damage to the health of a data subject; or
- part of the Personal Data held on a public register; or
- authorised by the Data Protection Commissioner, which is normally the approval of a contract which is based on EU model contracts; or
- has provided appropriate safeguards through a legal transfer mechanism; or
- the recipient country or the recipient international organisation in question has been deemed by the European Commission to have an adequate level of protection and that adequate legal remedy is available to the data subjects.

In addition, IACAT will ensure that data subjects are made aware that their data may be transferred outside the EEA. Where the data being transferred is Special Category Data it will be necessary to obtain the Data Subject's explicit consent to any form of processing, including transfers abroad.

Note: the transfer of data outside the EEA may include situations where a third party **provides remote access or transfers** IACAT data to another geographical location outside the EEA. The situation may also arise where a third party provides remote access or transfers IACAT data to an external party **outside the EEA** to whom it outsources particular functions, such as a cloud provider for example. IACAT as the Data Controller is ultimately responsible for the Personal Data it transfers to the remit of these external parties **and, must satisfy one of the conditions above**.

Compliance with this section will be addressed by the Data Protection Responsible Person in the event of any proposed transfer of data beyond the EEA. The Data Protection Responsible Person must be contacted in the event that a transfer of data outside of the EEA is necessary.

IACAT's policy is to minimise the transfer of Personal Data outside the EEA.

9 Document Ownership

The owner of this document is the Data Protection Responsible Person.

10 Maintenance

This Data Protection Policy is reviewed on an annual basis or in light of any legislative or other relevant developments.

11 Enforcement

The Applicable Data Protection Legislation has provision for the imposition of penalties for failures to comply and provision for data subjects to bring a claim for compensation against an organisation found in breach of the Applicable Data Protection Legislation.

The **DPC** oversees national compliance with the terms of the legislation. The **DPC** has powers to investigate any complaints from data subjects and has the power to audit IACAT on foot of complaints or under its general powers to audit organisations.

The DPC is granted powers under the GDPR to administer fines of up to 4% of turnover or €20,000,000, whichever is greater.
There is also a risk that Data Controllers in breach of the Applicable Data Protection Legislation **will be named in the DPC's Annual Report which can reflect badly on** IACAT**.**

In relation to unsolicited marketing by electronic means, summary proceedings for an offence under S.I. No. 336 of 2011 may be brought and prosecuted by the Commissioner.

Each call or message can attract a fine of up to €5,000 on summary conviction. If convicted on indictment, the fines range from €50,000 for a natural person to €250,000 or 10% of turnover if the offender is a corporate body.

Data Subjects who are not happy with any aspects of how their Personal Data is processed by IACAT may lodge a complaint with the DPC by emailing them on info@dataprotection.ie or by completing their online form on their website https://www.dataprotection.ie/

12 References

For further details relating to the following legislation please refer to the **DPC**'s website www.dataprotection.ie:

- The Data Protection Acts 1988-2018
- Statutory Instrument S.I. No.336 of 2011 The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011
- General Data Protection Regulation EU 2016/679

13 Definitions

For the purposes of this document the following definitions apply:

Data Protection	Data protection is the safeguarding of the fundamental privacy rights and freedoms of individuals in relation to the processing of their Personal Data.
Data Controller	A Data Controller is a body that, either alone or with others, controls the contents and use of Personal Data. For the purposes of this policy, the Data Controller is IACAT As such, IACAT is ultimately responsible for ensuring that any third party or external party, to which the processing of Personal Data is outsourced, comply with the Applicable Data Protection Legislation.
Data Processor	A data processor refers to a person or third party who processes Personal Data on behalf of a Data Controller. All Data Processors who process Personal Data on behalf of IACAT must only process the data in accordance with the written instructions of IACAT and must ensure that the data is kept safe and secure at all times.
Third Party	A third party refers to an organisation that holds a contract with IACAT and is a direct supplier of services and/or software to IACAT.
External Party	An external party refers to an organisation that does not have a contract with IACAT but provides services to a third party which involves the processing of IACAT Personal Data on behalf of the third party.
Users	Users refer to IACAT personnel, contract and agency staff, consultants, advisors and agents, who process Personal Data in either paper or electronic format on behalf of IACAT.
Data Subject	Data Subject means an individual who is the subject of Personal Data.
Personal Data	Personal Data means any information relating to an identified or identifiable natural person ("data subject").
Special Category Data	Relates to specific categories of Personal Data such as: • The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the Data Subject; • **Whether the Data Subject is a member of a trade union;** • Genetic data or biometric data; and • The physical or mental health or condition or sexual life of the Data Subject;
Processing	Processing means performing any operation or set of operations on the Personal Data or on sets of Personal Data, whether or not by automatic means, including: • Obtaining, recording or keeping the information, • Collecting, recording, organising, storing, altering or adapting the information or data, • Retrieving, consulting or using the information or data • Disclosing the information or data by transmitting, disseminating or otherwise making them available, or • Aligning, combining, blocking, erasing or destroying the information or data.