During periods of emergency, including national pandemics, please contact ICA directly for changes to its current policies and processes (T: 823789 or E: office@islandcommunityaction.org.uk)

POLICY 7: GENERAL DATA PROTECTION REGULATION POLICY (UK GDPR)

1. Introduction

The aim of the ICA UK GDPR Policy is to ensure employees and volunteers (includes trustees) are not only fully aware of the standards of work and performance expected of them but are also supported to deliver against these standards.

2. Policy Statement

ICA recognises that a key priority under UK GDPR is to avoid causing harm or distress to any individual.

As such, it is essential that any information held about its employees, volunteers and clients is used fairly, held securely and not disclosed to any other person unlawfully.

ICA also recognises that its employees and volunteers are consistently called upon to process personal data about other individuals. As such, ICA has a responsibility for ensuring that all such interactions with personal data:

2.1. Comply with both the law and good practice

2.2. Respect individuals' rights

2.3. Be open and honest with individuals whose data is held

2.4. Provide training and support for employees and volunteers who handle personal data, so that they can act confidently and consistently.

In addition, ICA is committed to ensuring that:

2.5. Any disciplinary action taken related to data protection will follow the process detailed in ICA's Disciplinary Policy

2.6. All matters relating to or arising under ICA's Disciplinary Policy must be treated as confidential at all times, with failure to do so constituting grounds for further disciplinary action.

3. Data Protection Principles

ICA is committed to processing data in accordance with the responsibilities outlined in Section 5 and its responsibilities under the UK GDPR.

The UK GDPR requires that personal data shall be:

3.1. Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')

3.2. Collected for specified, explicit and legitimate purposes and not further processed 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 ('purpose limitation')

3.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

3.4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

3.5. 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 the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')

3.6. 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 ('integrity and confidentiality')."

4. Definitions

4.1. The Data Subject is the individual whose personal data is being processed. Examples include:

- **4.1.1.** Employees – past / present
- **4.1.2.** Volunteers
- **4.1.3.** Clients
- **4.1.4.** Donors
- **4.1.5.** Sessional workers
- **4.1.6.** Suppliers
- **4.1.7.** Job applicants.

4.2. Contact Information means any or all of the data subject's: full name (including any preferences about how they like to be called); full postal address; telephone and/or mobile number(s); e-mail address(es), social media IDs / user-names (*e.g.* Facebook, Twitter, WhatsApp).

4.3. Processing means the use made of personal data including:
- **4.3.1.** Obtaining and retrieving
- **4.3.2.** Holding and storing
- **4.3.3.** Making available within or outside the organisation
- **4.3.4.** Printing, sorting, matching, comparing and destroying.

4.4. The Data Protection Officer (DPO) is the name given to the person in organisations who is the central point of contact for all data compliance issues. ICA's DPO is its Chief Executive Officer (CEO).

5. Responsibilities

5.1. ICA's Board of Trustees (BoT) recognises its overall responsibility for ensuring that ICA complies with its legal obligations.

5.2. ICA's DPO is the central point of contact for data compliance issues.

5.3. ICA's DPO has the following responsibilities:

- **5.3.1.** Briefing the BoT and employees on UK GDPR responsibilities (employees will be responsible for informing volunteers through their induction and ongoing training).
- **5.3.2.** Reviewing UK GDPR and related policies.
- **5.3.3.** Handling subject access requests.
- **5.3.4.** Approving unusual or controversial disclosures of personal data.
- **5.3.5.** Ensuring contracts with data processors have appropriate data protection clauses.
- **5.3.6.** Electronic security.
- **5.3.7.** Approving data protection-related statements on materials and letters.

5.4. Employees and volunteers at ICA who handle personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good data protection practice is established and followed.

5.5. Employees and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

5.6. Significant breaches of this policy will be handled under ICA's disciplinary procedures **(See ICA's Disciplinary Policy for more information)**.

6. Lawful, Fair And Transparent Processing

6.1. To ensure its processing of data is lawful, fair and transparent, ICA shall maintain a Register of Systems **(See Appendix 1: Register of Systems)**.

6.2. The Register of Systems shall be reviewed at least annually.

6.3. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

7. Lawful Purposes

In order for ICA to obtain, hold and process personal information, one of the six lawful purposes listed below must apply – for all purposes the information held and processed will include the contact information listed in point 4.2. above (+ any additional information listed against the individual purpose).

7.1. By Consent – For instances where people are interested in and wish to be kept informed about ICA's activities and services.

Subject to the person's consent, the information provided by ICA may also include details about activities relevant to ICA but run by other organisations (this will not involve sharing personal data to other organisations).

The information collected may also contain details of any particular areas of interest held by the person.

Information will be held and processed solely for the purpose of providing the information requested by the person.

7.2. By Contract – For instances where people sell goods and / or services to, and / or purchase goods and / or services from ICA.

The information collected will additionally contain details of:

7.2.1. The goods / services being sold to, or purchased from ICA.

7.2.2. Bank and other details necessary and relevant to the making or receiving of payments for the goods / services being sold to or purchased from ICA.

Information will be held and processed solely for the purpose of managing the contract between ICA and the person supplying or purchasing goods.

7.3. By Legal Obligation – For instances where there is a legal obligation on ICA to collect, process and share information with a third party. For example, the legal obligations to collect, process and share an employee's payroll information with HM Revenue & Customs (e.g. NI number, taxation codes, salary details, benefits, tax and NI deductions and pension payments.

Information will be held, processed and shared with others solely for the purpose meeting ICA's legal obligations.

7.4. By Vital Interest – For instances where the processing of information is necessary to protect someone's life. For example, ICA collecting the name and contact number of an emergency contact for each client.

7.5. By Public Task – For instances where the processing of information is necessary for ICA to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

7.6. By Legitimate Interest – For instances where, in order to be able to operate efficiently, effectively and economically, it is in the legitimate interests of ICA to hold such personal information on its volunteers as will enable it to communicate with them on matters relating to its operation, including meetings, information about ICA's activities, consultation / evaluation exercises and training opportunities etc.

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

8. Data Minimisation

8.1. ICA shall ensure that any personal data collected and processed should not be held or further used unless its use is essential and for reasons that were clearly stated **in** advance to support data privacy

9. Accuracy

9.1. All relevant systems will be updated should ICA become aware that information about any individual changes.

9.2. All relevant systems will be updated should ICA becomes aware that information about any individual is inaccurate.

10. Archiving / removal

All information related to the archiving and removal of data can be found in the Register of Systems.

11. Security

This section of the policy addresses security issues relating to personal data and not security of the building, business continuity or any other aspect of security.

The points outlined below provide an overview of processes, with all detailed information being outlined in ICA's Register of Systems.

11.1. General non-confidential information about organisations will be kept in unlocked filing cabinets or computer files with open access to all ICA employees and volunteers.

11.2. ICA shall ensure that personal data is stored securely.

11.3. Access to personal data shall be limited solely to those who need access and appropriate security should be in place to avoid any unauthorised sharing of information.

11.4. Employees and volunteers should be careful about information that is displayed on their computer screen and must make every effort to ensure that no unauthorised person can view the data when it is on display.

11.5. Data about any ICA employee, volunteer or client will be held in as few places as necessary, with all employees and volunteers being discouraged from establishing unnecessary additional data sets.

11.6. Back-up and data recovery solutions shall be in place, with employees and volunteers responsible for backing-up data related to their work.

11.7. Employees and volunteers who must keep more detailed information about any individual will be given additional guidance re appropriate storage.

11.8. In an emergency situation, the trustees and CEO may authorise access to files by other people.

12. Confidentiality

12.1. Because confidentiality applies to a much wider range of information than data protection, ICA has a separate Confidentiality Policy. ICA's UK GDPR Policy should be read in conjunction with ICA's Confidentiality Policy.

12.2. ICA has also has a Privacy Statement for clients, setting out how their information will be used. This is available on request **(See Appendix 2: Privacy Statement).**

12.3. Employees and volunteers will sign a short statement indicating that they have been made aware of their confidentiality responsibilities.

12.4. In order to provide some services, ICA may need to share client's personal data with other agencies (Third Parties). Verbal or written agreement will always be sought from the client before data is shared.

12.5. Where anyone within ICA feels that it would be appropriate to disclose information in a way contrary to the Confidentiality Policy or where an official disclosure request is received, this will only be done after discussions with ICA's DPO. All such disclosures will be documented.

13. Access

13.1. All clients and other customers have the right to request access to data stored about them. Access requests should be handled by ICA's DPO, with a response to the requester being made within the legal timeframe of 30 days.

13.2. The request from clients must be made in writing (hard copy or digital) to the ICA's DPO.

13.3. Where the individual making a request is not personally known to ICA's DPO their identity will be verified before handing over any information.

13.4. The required information will be provided to the clients in a permanent form unless the applicant makes a specific request to be given supervised access in person.

13.5. ICA will provide details of information to clients who request it unless the information may cause harm to another person.

13.6. Employees and volunteers have the right to request access to data stored about them. Access requests should be handled by ICA's DPO, with a response to the requester being made within 14 days.

NB: If information held is inaccurate, the individual must notify ICA's DPO or BoT Chair so that this can be recorded on file.

13.7. The request from employees and volunteers must be made in writing (hard copy or digital) to ICA's DPO.

13.8. Individual requests will be free of charge unless considered 'manifestly unfounded or excessive.'

A request may be considered 'manifestly unfounded' or 'excessive' if:

13.8.1. The individual clearly has no intention to exercise their right of access. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from ICA.

13.8.2. The request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption.

13.8.3. It repeats the substance of previous requests and a reasonable interval has not elapsed

13.8.4. It overlaps with other requests.

14. Transparency

14.1. ICA is committed to ensuring that in principle Data Subjects are aware that their data is being processed and also:

- **14.1.1.** For what purpose it is being processed
- **14.1.2.** What types of disclosure are likely, and
- **14.1.3.** How to exercise their rights in relation to the data.

14.2. Data Subjects will generally be informed in the following ways:

- **14.2.1.** Employees – in the staff terms and conditions
- **14.2.2.** Volunteers – in the volunteer welcome / support pack
- **14.2.3.** Clients – when they request services.

14.3. Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory.

15. Consent

15.1. Consent will normally not be sought for processing information about employees and volunteers for internal / work purposes. For external requests (e.g. financial references), however, consent will be sought.

15.2. Information about employees and volunteers will be made public according to their role requirements, however, consent will be sought regarding any information to be included that is not essential for their role.

15.3. Information about clients will only be made public with their consent (includes photographs).

15.4. 'Sensitive' data about clients (including health information) will be held only with the knowledge and consent of the individual.

15.5. Once given, consent can be withdrawn, but not retrospectively.

NB: There may be occasions when ICA has to retain data for a certain length of time, even though consent for using it has been withdrawn.

16. Direct Marketing

16.1. ICA will treat the following unsolicited communication as marketing:

- **16.1.1.** Seeking donations and other financial support
- **16.1.2.** Promoting ICA activities or services
- **16.1.3.** Promoting ICA events and other fundraising exercises
- **16.1.4.** Promoting membership to supporters.

16.2. Whenever data or contact information is first collected which might be used for marketing as well as contact purposes, this will be made clear and the Data Subject will be given a clear opt out of future marketing communications.

16.3. ICA currently has no policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.

17. Employee Training and Acceptance of Responsibilities

17.1. Data Protection will be included in the induction training of ICA employees and volunteers. This will include referencing all other relevant policies and procedures, including both the Data Protection and Confidentiality policies.

17.2. ICA will provide additional updates through training, meetings, and supervisions.

18. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, ICA shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

Main contact for issues related to ICA's UK GDPR Policy:
Kim Wilcocks, CEO
T: 01305 823789
E: office@islandcommunityaction.org.uk

LINKED POLICIES	
POLICYNUMBER	**POLICY TITLE**
1	Confidentiality Policy
2	Conflict of Interest Policy
3	Disciplinary Policy
4	Environmental Policy
5	Equal Opportunities Policy
6	Financial Procedures Policy
7	UK GDPR Policy
8	Grievance Policy
9	Health & Safety Policy
10	Lone Working Policy
11	Online Cookie & Privacy Policy
12	Risk Management Policy
13	Safeguarding_Children & Young People Policy
14	Safeguarding_Vulnerable Adults Policy
15	Training & Development Policy
16	Transport Policy
17	Whistleblowing Policy

APPROVAL

This policy was referred to and signed by the CEO and Chair of the Board of Trustees.

Date…31st March 2021… Review date…31st March 2022…

Chief Executive Officer……

Chair of Board Signature…….....

Appendix 1: Register of Systems

1. Introduction

In accordance with the General Data Protection Regulation, this Appendix sets out and reiterates the approach of ICA to the collection, use and management of the personal data of its members under the following headings:

1.1. The data we collect and in what way
1.2. How the data are stored and who has access to them
1.3. Sharing the data
1.4. Purpose for which the data are used
1.5. Data removal and archiving.

2. The data we collect and in what way

Those who engage with ICA in any meaningful way, including employees (past and present), volunteers, clients, donors, sessional workers, suppliers and job applicants, will be asked to provide information relevant to their engagement on a bespoke form created specifically for that engagement. These forms might include:

2.1. Volunteer registration forms
2.2. Client registration forms
2.3. Donor contact sheets
2.4. Sessional worker contact sheets
2.5. Supplier contact sheets
2.6. Job application forms

Templates for all forms can be accessed on request to an ICA employee.

Forms carry basic contact information, including name, residential or business address, telephone, email and health related data (where relevant).

Not all data from paper forms will be transferred to a digital format. Where necessary and in accordance with ICA's processes, however, relevant data will be entered on to digital forms, including Excel spreadsheets or Word documents (e.g. volunteer and client data is entered on to ICA's Evaluation Database for the purposes of aggregating usage data) by the relevant ICA employee or volunteer.

Such data will be updated whenever ICA becomes aware of changes (e.g. change of email or residential address).

Where relevant and consent has been given, names and email addresses shall also be entered on to digital documents (e.g. an Excel spreadsheet), used to facilitate the dispatch/receipt of ICA information and updates.

3. How the data is stored and who has access to them

Data is stored as follows:

3.1. Data recorded on paper will be kept in lockable cabinets, with files and filing cabinets bearing confidential information will be labelled 'Confidential'.

3.2. Data recorded digitally will be protected by password on a system that uses modern, up to date, software.

NB: ICA uses an Evaluation Database (Excel spreadsheet) to aggregate personal data and information related to service usage. This database is password protected and reviewed at regular intervals to make sure it is still fit for purpose.

4. Sharing data

The complete data set will be shared solely with ICA's employees and Data Volunteer.

The complete data set will not be shared with any third party unless consent is sought in advance from the Data Subject or ICA is legally obliged to do so.

Individual personal data will be shared with ICA's employees and relevant volunteers (e.g. those providing services, such as befrienders and drivers).

5. Purpose for which the data are used

ICA's data is processed on the basis of one of the purposes mentioned in **Section 7**:

5.1. Consent – the individual has given clear consent (e.g. a volunteer or client).

5.2. Contract – the processing is necessary for a contract you have with the individual (e.g. client).

5.3. Legal obligation – the processing is necessary for you to comply with the law (e.g. employee information to HMRC).

5.4. Vital interests – the processing is necessary to protect someone's life (e.g. client emergency contact details).

5.5. Public task – the processing is necessary for you to perform a task in the public interest function has a clear basis in law.

5.6. Legitimate interests – the processing is necessary for ICA's legitimate interests unless protection of the Data Subject overrides those legitimate interests.

6. Data removal and archiving

ICA will retain personal data for no longer than required. The duration varying according (e.g. to the type of engagement the Data Subject had with ICA or our funder's requirements etc.)

Appendix 2: Privacy Statement

When you request information from ICA, sign up to any of our services or buy things from us, ICA obtains information about you. This statement explains how we look after that information and what we do with it.

We have a legal duty under the UK General Protection Regulation Policy (UK GDPR) of 2018 to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally the only information we hold comes directly from you. Whenever we collect information from you, we will make it clear which information is required in order to provide you with the information, service or goods you need.

You do not have to provide us with any additional information unless you choose to.

We store your information securely in locked filing cupboards or on password protected electronic devices e.g. computers. We restrict access to those who have a need to know, and we train our employees and volunteers in handling the information securely.

If you have signed up to a class or other service we will also pass your details to the professional worker / volunteer providing that service. That worker / volunteer may hold additional information about your participation in these activities.

We would also like to contact you in future to tell you about other services we provide, to keep you informed of what we are doing and ways in which you might like to support ICA. You have the right to ask us not to contact you in this way. We will always aim to provide a clear method for you to opt out. You can also contact us directly at any time to tell us not to send you any future marketing material.

Very occasionally we may carry out a joint mailing with carefully selected other organisations, in order to tell you about products and services we think you might be interested in. Again, you have the right to opt out of this.

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you). To obtain a copy, you should put your request in writing to ICA's DPO (please see the foot of this page for our address).

As previously stated **(See Section 13.8)**, there is no charge for a copy of your data unless the request is *'manifestly unfounded or excessive,'* or you have made multiple requests. If a fee is to be charged, we will advise you of this beforehand.

We aim to reply within one month (the legal maximum time permitted). However, if the request is complex or you have made multiple requests, we may take up to two months longer. Again, we will advise you of any delay beforehand.