ICA:UK Privacy (Data Protection) Policy

This policy replaces ICA:UK's Data Protection Policy (2011) after substantive review due to the introduction of the General Data Protection Regulations (GDPR), effective 25th May 2018

(Sources: This policy has been compiled from various sources, including ICO and EUDPR guidance, and based on a template produced by Clarity CIC (http://www.claritycic.org/))

Date: Approved by the ICA:UK Board 17th September 2018
Due for Review: September 2020

ICA:UK is a company limited guarantee (No. 3970365) and registered charity (No. 1090745) This privacy policy explains what personal information we gather, how we use it, and why. It also sets out individual's rights in relation to that information, and explains the processes which individuals can use to exercise those rights.

The policy seeks to show ICA:UK's commitment to the six GDPR principles:

1. Lawfulness, fairness and transparency
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

2. Purpose limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

3. Data minimisation
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. Accuracy
Personal data shall be accurate and, where necessary, kept up to date

5. Storage limitation
Personal data shall be 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

6. Integrity and confidentiality
Personal data shall be 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.

1. Data protection responsibility and Accountability

a) The responsibility of Data Protection and GDPR compliance lies with the ICA:UK Board of Trustees who are responsible for implementing the policy and monitoring compliance and ensuring the information is made accessible and communicated to all staff and volunteers
b) The ICA:UK Board of Trustees will review and update the policy at two-year intervals or when required to ensure it remains relevant.
c) We will regularly test measures that are detailed within the policies to provide assurances about their continued effectiveness
d) The Director of ICA:UK is responsible and accountable to the Board for enabling ICA:UK to meet the GDPR obligations. This includes
    i. informing the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
    ii. monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, awareness raising and training of staff and conducting internal audits
    iii. advise on and monitor data protection impact assessments
    iv. act as the contact point for, and to cooperate with the ICO, and to consult on any data protection matter; and
    v. ensuring there is a contact point for individuals whose data is processed (employees, customers etc).

2. Data Protection by Design

We aim to adopt internal policies and implement measures which help us comply with the data protection principles

a) Data security systems

We will process personal data in a manner that ensures appropriate security.

i. To do this we will decide what level of security is right for our organisation and assess the risks to the personal data we hold and choose security measures that are appropriate to our needs**.**
ii. When processing personal data within our IT system(s) we will recognise the risks involved and take appropriate technical and organisational measures to secure the data.
iii. We will keep our IT systems safe and secure and ensure we provide adequate time, resource and (potentially) seek specialist expertise.

b) Information risks and mitigation

The ICA:UK Board of Trustees, working through the Director, are responsible for managing information risks, coordinating procedures put in place to mitigate them and for logging and risk assessing information assets. Where we have identified information risks, we have appropriate action plans in place to mitigate any risks that are not tolerated or terminated

c) Breach notification

We understand we have a duty to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.(*A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data).*

i. We will notify the ICO of a breach within 72 hours (unless it is unlikely to result in a risk to the rights and freedoms of individuals).
ii. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify those concerned directly and without undue delay.
iii. In all cases we will maintain records of personal data breaches, whether or not they are notifiable to the ICO.

d) Information we hold

We maintain an **information asset register** with details of what personal data we hold, where it came from, who we share it with and what we do with it.

3. Data Quality

a) We will regularly review the information we process or store to identify when we need to take action, e.g. correct inaccurate records.
b) We will use Records management policies, with rules for creating and keeping records (including emails) where it is deemed useful.
c) We will use data quality reviews of systems and manual records we hold to ensure the information continues to be adequate for the purposes we originally collected it

4. Retention of Personal Data

We retain personal data according to the following guidance:

a) Employees: as set out in our Human Resources Policy
b) External contracts: for three years after the end of the contract
c) Third Parties we engage with (e.g. trainees, Associates, clients): for three years after any engagement (unless otherwise requested)
d) Where financial transactions are involved, HMRC requires we hold data for six years after the end of the Financial Year in which the transaction takes place.

5. Lawful basis for processing personal data

We keep personal data under the following basis:

a) **Consent**: the individual has given clear consent for us to process their personal data for a specific purpose.
b) **Contract**: the processing is necessary for a contracts we hold with individuals, or because they have asked us to take specific steps before entering into a contract.
c) **Legal obligation**: the processing is necessary for us to comply with the law (not including contractual obligations).
d) **Legitimate interests**: the processing is necessary for our legitimate interests or the legitimate interests of a third party

6. Sensitive Data

ICA:UK's values seek to work with all people. We therefore do not actively seek or retain sensitive data as defined by the GDPR (Article 9) (e.g. racial or ethnic origin; political opinions; religious or

philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data; biometric data where processed to uniquely identify a person)

7. Consent

Where required, we seek consent from people when collecting and retaining personal data and offer people genuine choice and control over how we use their data. We do this by:

a) Keeping our consent requests prominent and separate from our other terms and conditions.
b) Seeking a positive opt-in such as unticked opt-in boxes or similar active opt-in methods.
c) Avoiding making consent a precondition of service.
d) Being specific and granular- Allow individuals to consent separately to different purposes and types of processing wherever appropriate.
e) Naming our business and any specific third party organisations who will rely on this consent.
f) Keeping records of what an individual has consented to, including what you told them, and when and how they consented.
g) Telling individuals they can withdraw consent at any time and how to do this.
h) We continue to review consent as part of our ongoing relationship with individuals to ensure we meet GDPR's standards

8. Legitimate interests

(Legitimate interest applies to (e.g.) holding past data on people who have accessed services and whom we keep records for marketing/training/research purposes)

Where we have a **Legitimate interests** in holding personal information we will undertake a review to ensure we use people's data in ways they would reasonably expect. We will do this by considering:

Firstly:

i. Why do we want to process the data – what are we trying to achieve?
ii. Who benefits from the processing? In what way?
iii. Are there any wider public benefits to the processing?
iv. How important are those benefits?
v. What would the impact be if we couldn't go ahead?
vi. What are the dangers of the data being used in an unethical or unlawful in any way?

Secondly, we would apply the **necessity tests**.

i. Does this processing actually help to further that interest?
ii. Is it a reasonable way to go about it?
iii. Is there another less intrusive way to achieve the same result?

Thirdly, we would do **a balancing test** by:

i. Consider the impact of processing and whether this overrides the interest we have identified.
ii. What is the nature of our relationship with the individual?
iii. Is any of the data particularly sensitive or private?
iv. Would people expect we to use their data in this way?
v. Are we happy to explain it to them?
vi. Are some people likely to object or find it intrusive?

vii. What is the possible impact on the individual?
viii. How big an impact might it have on them?
ix. Are we processing children's data?
x. Are any of the individuals vulnerable in any other way?
xi. Can we adopt any safeguards to minimise the impact?
xii. Can we offer an opt-out?

9. International

By the nature of our work and our connections with third parties and other members of the ICA International network, ICA:UK is involved with some cross-border processing of data with countries both within and outside the EU. In this regard we operate under the UK supervisory body (ICO) and will apply the same safeguards to all our data.

10. Individuals Rights

We are aware that individuals have a right to be informed that we are collecting their data, why we are processing it and who we are sharing it with. To make sure individuals know this we will publish privacy information on our website and within any forms or letters we send to individuals. The information will be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge

The information we supply will depends on whether we obtained the personal data directly from the individual or a third party.

11. Right of Access

We acknowledge the right of individuals to have access to their data and will provide a copy of the information we hold about them within one calendar month of receiving it free of charge (unless in exceptional circumstances i.e. manifestly unfounded or excessive, in which case we may charge an admin fee)

12. Right to rectification

a) We will respond to a request for information to be rectified within one month of receipt (this may be extended to two months in exceptional circumstances - in which case we will contact the person making the request).
b) We will verify the identity of the person making the request, using "reasonable means".
c) Where possible – where we have shared the personal data with other organisations (for example other controllers or processors) we will inform them of the need for rectification

13. Right to erasure including retention

a) We recognise the right of Individuals have to be forgotten and will respond to requests for the erasure of personal data within one month of receipt (this may be extended by up to two months in exceptional circumstance - in which case we will contact the person making the request)
b) We will verify the identity of the person making the request, using "reasonable means".

c) On occasions we may refuse to comply with a request for erasure if we are processing the personal data for the following reasons:
    i. to exercise the right of freedom of expression and information;
    ii. to comply with a legal obligation ;
    iii. to perform a public interest task or exercise official authority;
    iv. for archiving purposes in the public interest, scientific research historical research or statistical purposes; or
    v. to exercise or defence of legal claims;

14. Right to restrict processing

We recognise the right of Individuals have to block or restrict the processing of their personal data and will respond to requests to restrict the processing of their personal data within one month of receipt.

a) Whilst investigating the right for restriction we will only store the personal data, but not further process it.
b) We will retain just enough information about the individual to ensure that the restriction is respected in the future.
c) We will consider restricting the processing of personal data if:
    i. an individual contests the accuracy of the personal data, (we will restrict the processing until we have verified the accuracy of the personal data).
    ii. an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual.
    iii. processing is unlawful and the individual opposes erasure and requests restriction instead.
    iv. we no longer need the personal data but the individual requires the data to be retained to allow them to establish, exercise or defend a legal claim.
    v. If we have disclosed the personal data to other organisations (controllers or processors), we will inform them about the restriction, unless it is impossible or involves disproportionate effort to do so.
    vi. We will inform individuals when we decide to lift a restriction on processing.

15. Data Portability

We recognise the right of Individuals have to their data portability and will enable individuals to obtain and reuse their personal data for their own purposes across different services and will respond to requests for personal data free of charge within one month of receipt

a) The right to data portability only applies:
    i. to personal data an individual has provided to us as a controller;
    ii. where the processing is based on the individual's consent or for the performance of a contract; and
    iii. where the processing is carried out by automated means. Individuals can make a request verbally or in writing.
b) We will verify the identity of the person making the request, using "reasonable means".

c) We will provide the personal data in a structured, commonly used and machine readable format. Examples of appropriate formats we will use include CSV and XML files.
d) If the individual requests it, we may transmit the data directly to another business where this is technically feasible.

16. Right to Object

We recognise the right of Individuals have a right to object having their data collected/ retained in certain circumstances and will respond to requests made verbally or in writing within one month of receipt

a) We will inform individuals of their right to object "at the point of first communication" and present it separately from other information on rights clearly laid out in our privacy notice.
b) We will verify the identity of the person making the request, using "reasonable means".
c) We will stop processing data for any direct marketing as soon as we receive an objection
d) Occasionally we will process personal data for the purposes of scientific/historical research purposes or statistical purposes. In this case we will seek consent and may refuse the right to object if the processing is necessary for the performance of a task carried out for reasons of public interest