

## Data Protection Policy

---

The ICE Benevolent Fund is the data controller for the purposes of the EU General Data Protection Regulation (GDPR).

ICE Benevolent Fund's Data Privacy Manager is Mrs. Kris Barnett, tel: 01444 417 979/email: kris.barnett@icebenfund.com. Any queries regarding ICE Benevolent Fund's Data Protection Policy should be addressed to her.

### What is Personal Data

Personal Data is data which relates to a living individual who can be identified. Sensitive personal data (special category data under GDPR) includes data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, data concerning physical or mental health or finances.

### Personal Data Processed by ICE Benevolent Fund

---

Data protection issues apply not only to relevant computer systems and programmes, but also to all records (including structured paper filing systems) if they contain personal information about an individual.

The ICE Benevolent Fund maintains a range of data on ICE members and their families, including personal and financial information, health and wellbeing information, professional history, engineering specialisms, professional development and interests. This information will be stored securely and processed lawfully for the following individuals:

- **ICE Members** - specifically ICE Benevolent Fund Members, ICE Benevolent Fund Visitors, ICE Benevolent Fund Trustees
- **Dependents of ICE members** who are eligible for support from the ICE Benevolent Fund

The ICE Benevolent Fund also maintains data on other categories of individuals, but the data retained for these categories is not classed as special category data and will include:

- **Benevolent Fund Staff**  
Name, address and full contact details and next of kin details, so that contact can be made at home in an emergency
- **Non-members**  
Names, addresses and full contact details of suppliers/partners/contractors with whom the Benevolent Fund does business.



## **Who will have access to the personal information?**

ICE member, dependent of ICE member, non-member and staff information will be accessed, reviewed and used by the Ben Fund's staff.

Ben Fund Trustees will review the personal information (including sensitive personal information) of applicants and beneficiaries of the ICE Benevolent Fund, but identifying details will never be disclosed. All application and beneficiary cases considered by Trustees are anonymised.

Contact details and sensitive personal information may be passed to an applicant or beneficiary's local visitor for the visitor to make contact and provide local support, but this will only be done with an applicant or beneficiary's specific consent.

The information may also be passed to trusted third parties for assessing need and the provision of additional support only. Individuals in receipt of additional support will sign separately to indicate their willingness for personal information to be shared with trusted third parties.

Information will never be passed to a third party for marketing purposes without specific permission.

## **Data Protection Principles**

All personal data must be dealt with in accordance with the six data protection principles set out in the GDPR which are shown below with issues arising.

---

### **All data must be processed fairly, lawfully and in a transparent manner and it will only be lawful if one of the processing conditions is met**

1. All personal information must be obtained by The ICE Benevolent Fund in a way that does not deceive or mislead data subjects as to how their information will be used. All Data subjects must be provided with the required privacy statement information under GDPR ("Privacy Notice"). New applicants to ICE Benevolent Fund are asked to confirm that they have read and understood the ICE Benevolent Fund's Privacy Notice.

---

### **All data must be obtained and processed only for specified and limited purposes**

2. The ICE Benevolent Fund can only process personal data in a manner consistent with the purposes for which it was obtained. It must not be used for any other purpose beyond this without informing the individual and complying with the rest of the principles.



**All data must be adequate, relevant and not limited to what is necessary for the purpose for which it was collected**

3. The ICE Benevolent Fund will not obtain any surplus or unnecessary personal data from a Data subject. All personal data will be screened and assessed – is this information really required? Aside from compliance with data protection legislation, it is good working practice to keep only the minimum amount of information necessary to operate efficiently.

---

**All data must be accurate and, where necessary, updated**

4. All data held by the ICE Benevolent Fund will be accurately recorded and kept up to date. If personal data held by the ICE Benevolent Fund is incorrect or has changed, all records and files should be updated as soon as possible. It is acceptable to annotate any incorrect or misleading information to indicate the inaccuracy (or any challenge to the accuracy) rather than amending the original text – if in doubt contact the Data Privacy Officer.

- 
5. Data will be kept in line with the ICE Benevolent Fund's Data Retention Policy.

- 
6. The ICE Benevolent Fund is obliged to take appropriate organisational and technical measures to keep all personal data secure.

ICE Benevolent Fund will take reasonable steps to ensure that members of staff [and volunteers] will only have access to personal data where it is necessary for them to carry out their duties. All staff [and volunteers] will be made aware of this Policy and their duties under the GDPR. The Charity will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons. For further details as regards security of IT systems, please refer to the Information, Communication, Technology (ICT) policy.

---

**Transfers outside of the EEA**

All data must not be transferred out of the European Economic Area ("EEA") without appropriate safeguards

We recognise that personal data needs to be treated with particular care in countries which do not have reciprocal data protection laws.



## **The conditions for processing personal data under the first data protection principle**

- The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given;
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regard to entering into a contract with the individual, at their request;
- The processing is necessary for the performance of a legal obligation to which we are subject;
- The processing is necessary to protect the vital interests of the individual or another;
- The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us;
- The processing is necessary for a legitimate interest of ICE Benevolent Fund or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned. More details of this are given in the Privacy Notice, where applicable.

## **Disclosure of Personal Data**

The following list includes the most usual reasons that ICE Benevolent Fund will authorise disclosure of personal data to a third party:

- to give a confidential reference relating to a current or former employee;
  - for the prevention or detection of crime;
  - for the assessment of any tax or duty;
  - where it is necessary to exercise a right or obligation conferred or imposed by law upon us (other than an obligation imposed by contract);
  - for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
  - for the purpose of obtaining legal advice;
  - for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- ICE Benevolent Fund may receive requests from third parties (i.e. those other than the data subject, the charity, and its employees) to disclose personal data it holds about individuals. This information will not generally be disclosed unless one of the specific exemptions under the GDPR which allow disclosure applies, or where disclosure is necessary for the legitimate interests of the third party concerned or the charity.
  - All requests for the disclosure of personal data must be sent to Data Privacy Manager, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of the requesting third party before making any disclosure.



## **Rights of Data Subjects**

Data subjects are given substantial rights under the GDPR. It is therefore vital that all requests and enquiries from data subjects are logged and reported to the Data Privacy Manager as soon as possible. An individual may be entitled to see what has been recorded about them.

ICE Benevolent Fund is committed to ensuring that anyone dealing with personal data shall be mindful of the individual's rights under the law.

All data must be kept securely to avoid accidental loss, destruction or damage to personal data.

## **Subject Access Requests**

Anybody who makes a request to see any personal information held about them by the ICE Benevolent Fund is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system".

A subject access request must be made in writing. ICE Benevolent Fund may ask for any further information reasonably required to locate the information.

All requests should be sent to the Data Privacy Manager within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Data Privacy Manager must, however, be satisfied that:

- the child or young person lacks sufficient understanding; and
- the request made on behalf of the child or young person is in their interests.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances ICE Benevolent Fund must have written evidence that the individual has authorised the person to make the application and the Data Privacy Manager must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).



An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the Data Privacy Manager before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

### **Other rights of individuals**

The Charity has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the Charity will comply with the rights to:

- object to processing;
- rectification;
- erasure; and
- data portability.

### **Right to object to processing**

- An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (please see conditions for processing above)) where they do not believe that those grounds are made out.
- Where such an objection is made, it must be sent to the Data Privacy Manager within 2 working days of receipt, and the Data Privacy Manager will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.
- The Data Privacy Manager shall be responsible for notifying the individual of the outcome of their assessment within [Insert reasonable number] of working days of receipt of the objection.
- Where personal data is being processed for direct marketing purposes an individual has the right to object at any time to processing of personal data concerning him or her for such marketing (which includes profiling to the extent that it is related to such direct marketing) and their personal data shall no longer be processed by the ICE Benevolent Fund for direct marketing purposes.



## **Right to rectification**

- An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the Data Privacy Manager within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.
- Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual.
- An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

## **Right to erasure**

- Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:
  - where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
  - where consent is withdrawn and there is no other legal basis for the processing;
  - where an objection has been raised under the right to object, and found to be legitimate;
  - where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
  - where there is a legal obligation on the charity to delete.
- The Data Privacy Manager will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

## **Right to restrict processing**

In the following circumstances, processing of an individual's personal data may be restricted:

- where the accuracy of data has been contested, during the period when ICE Benevolent Fund is attempting to verify the accuracy of the data;
- where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;



- where there has been an objection made under the right to object above, pending the outcome of any decision.

### **Right to portability**

- If an individual wants to send their personal data to another organisation they have a right to request that you provide their information in a structured, commonly used, and machine-readable format. If a request for this is made, it should be forwarded to the Data Privacy Manager within 2 working days of receipt, and the Data Privacy Manager will review and revert as necessary.

### **Breach of the GDPR**

- Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Data Privacy Manager.
- Once notified, the Data Privacy Manager shall assess:
  - the extent of the breach;
  - the risks to the data subjects as a consequence of the breach;
  - any security measures in place that will protect the information;
  - any measures that can be taken immediately to mitigate the risk to the individuals.
- Unless the Data Privacy Manager concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Charity, unless a delay can be justified.
- The Information Commissioner shall be told:
  - details of the breach, including the volume of data at risk, and the number and categories of data subjects;
  - the contact point for any enquiries (which shall usually be [the Data Privacy Manager]);
  - the likely consequences of the breach;
  - measures proposed or already taken to address the breach.
- If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Privacy Manager shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.
- Data subjects shall be told:
  - the nature of the breach;
  - who to contact with any questions;
  - measures taken to mitigate any risks.
- The Data Privacy Manager shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the [board] and a decision made about implementation of those recommendations.





## **Other Issues**

The ICE Benevolent Fund's Data Privacy Manager will deal with all communications with regulators.

Kris Barnett  
Jan 2018