THE INTER FAITH NETWORK FOR THE UK

DATA PROTECTION POLICY

1. INTRODUCTION

The Inter Faith Network for the UK (**IFN**) has a responsibility to ensure that it uses personal data in accordance with the law. As such IFN has developed this Data Protection Policy (**Policy**). IFN staff, volunteers and trustees are accountable for upholding the Policy's requirements. Where data is made available to particular member bodies or categories of member body it will be so within previously stated usage parameters and subject to their agreement to use such data in keeping with UK GDPR requirements.

This Policy covers use of personal data about the categories of individual identified in section 2.5 below. IFN must comply with the Rules set out in this Policy about how it uses personal data. No Trustee, staff member, volunteer is exempt from compliance with these Rules.

This Policy does not form part of any employee or volunteer contract and may be amended at any time. Staff and volunteers and trustees will be notified of any significant changes.

If you have any questions about the matters outlined in this Policy, you should address these to the Executive Director in the first instance (as indicated below). However, if the Executive Director is not available and your query is urgent and/or requires attention while the Executive Director is away (for example because it relates to a data security breach), please contact the Project Director.

STAFF, TRUSTEES AND VOLUNTEERS ARE REQUIRED TO FAMILIARISE THEMSELVES WITH THIS POLICY.

2. BACKGROUND

What is data protection law?

Data protection law gives people the right to control how their 'personal data' (any information that relates to them, such as name, contact details, allegations of criminal activity, preferences etc.) is used. It also places obligations on organisations that use personal data. If the data you are using is properly and fully anonymised data, then its use falls outside the scope of this Policy.

In the EU, data protection law means the General Data Protection Regulation EU 2016/679 (**GDPR**) plus local data protection law that applies in each EU country. Although the UK is no longer part of the EU, the provisions of the GDPR have been automatically adapted into domestic UK law under the **UK GDPR**. IFN may be required to comply with both the UK GDPR and the (EU) GDPR depending on its activities.

What are we doing about it?

IFN treats compliance with its obligations very seriously. We have developed this Policy to ensure that the personal data we collect and use is done so in accordance with applicable data protection laws.

What are the consequences if we get it wrong?

Getting it wrong is serious, and could lead to complaints from individuals, compensation claims, fines from regulators and negative publicity. If any person deliberately fails to observe this Policy IFN will consider disciplinary action against them where appropriate.

Why is this policy important for IFN?

It is vital that those working, volunteering or serving as trustees as part of IFN observe this Policy because the collection and use of personal data is part of IFN's everyday business. IFN must ensure that it uses the information it holds on those identified in section 2.5 below in accordance with the law.

What types of personal data does IFN collect?

IFN collects personal data relating to:

- Applicants, employees and contractors (past and current) in connection with their (potential) role within IFN including (where relevant) contact details, DOB, next of kin, bank details, appraisal notes, CV, professional development, personnel file, benefits, compensation etc.
- (Past, current and prospective) Volunteers and trustees including contact details, DOB, and (for volunteers) next of kin;
- Service users in connection with the services we provide to them and to other service users;
- Donors
- Member body personnel for the management of the member relationship
- All other individuals we interact with (including, for example, subscribers to newsletters, event holders and attendees, and responders to surveys).

When should you collect and use personal data?

Collection and use of personal data must be in compliance with this Policy and the Rules set out below.

How does this Policy relate to other policies within IFN?

This Policy sits alongside IFN's Cyber Security Policy and Policy on use of personal devices for carrying out IFN work.

Want more information?

If you want more information about data protection and how the Rules affect IFN please contact the Executive Director (or the Project Director, if applicable).

3. THE RULES

Ensuring Transparency

The Rule: IFN must be transparent about the personal data that it holds on individuals including describing the purposes for which it uses personal data.

Understanding the Rule

Being transparent in the way that IFN uses and shares personal data is vital part of good data protection practice. For example, IFN is subject to this requirement in how it uses personal data on service users and employees – as such those individuals must be told how their personal data will be used.

There may be limited circumstances where we do not have to comply with the transparency requirement but you should check with the Executive Director before you proceed without ensuring transparency.

Practical Steps

Individuals will be provided with information about fair processing where personal data about them is being collected. For example, all employment contracts and the *Employee Handbook* will include suitable wording notifying the individual of how IFN will use their information.

If IFN offers individuals the opportunity to opt-out from or opt-in to receiving marketing or other uses of personal data, or the opportunity to access and correct personal data, such opportunities will be made clear, conspicuous and easy to use.

Collecting and using personal data for a lawful purpose only

The Rule: We must only collect and use the minimum amount of personal data which is necessary for one or more legitimate purpose which must be lawful and justifiable

Understanding the Rule

Personal data must only be collected or used (i) where it is relevant to IFN's business purposes (e.g. a HR purpose or for contract management), (ii) where IFN can rely on a lawful basis (or bases – see section 3.2.2 below), (iii) where the purposes are identified in the privacy notice provided to individuals, and (iv) where the collection and use is within the individual's expectations.

Practical Steps

When collecting personal data from individuals, IFN will ensure that the privacy notice made available to those individuals contains all of the purposes for which the personal data may be used.

In addition, when collecting personal data, IFN must only collect those details which are necessary for the purposes for which that personal data is being obtained. Any use of

personal data must be for the identified purposes and any different or new purposes should have a lawful basis. Personal data that is not necessary for any legitimate business purpose should not be collected or accessed. IFN staff, volunteers and trustees must not use any personal data accessed through their role for any private interest.

Can IFN rely on consent?

In some circumstances (though not always), use of personal data will require IFN to obtain the individual's consent. For instance, consent is often required in order to send marketing to individuals. But consent is not always an appropriate ground to rely on.

Consent is only valid if it is specific and informed so IFN must provide clear, unambiguous information on the purposes for which the personal data will be used when IFN collects consent. Consent must also be freely given so individuals must have a real choice about whether to provide their consent and must not be under pressure to consent.

It is important that IFN obtains documented evidence of the declaration of consent (e.g. in writing or via the use of an opt-in procedure). IFN's use of personal data must not exceed the purposes set out in the consent declaration and should not be used for different purposes.

Relying on explicit consent

In order to use certain types of data – known as special categories of data – IFN may need to obtain explicit consent from individuals. Special categories of data require additional protection. Special categories of data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or sex life or sexual orientation.

Explicit consent can be obtained where an individual is presented with a proposal to either agree or disagree to a particular use of his or her personal data and actively responds, either orally or in writing (which could be a wet ink signature on paper, or electronically through the use of an e-signature, clicking icons or sending confirmatory emails). But the need for explicit consent means it is not possible to construe implied consent through a person's actions.

What about the legitimate interest lawful basis?

UK GDPR allows processing of personal data where an organisation can rely on the legitimate interest lawful basis. It is not always obvious what this means and when IFN can rely on it. However, if IFN wishes to rely on the legitimate interest lawful basis it needs to be able to satisfy the test below:

1. Identify a legitimate interest for using personal data for a particular purpose. It could be our legitimate interest as an organisation or a third party's legitimate interest. For example: combating fraud, protecting network security, suppressing details on our marketing lists, direct marketing by mail etc.
2. Consider whether the processing of the personal data is necessary for satisfying that identified legitimate interest. Can IFN obtain the legitimate interest without processing personal data or could another less intrusive way be used?

3. Balance the legitimate interest IFN has identified with the rights and freedoms of the relevant individuals. Is IFN sure that their rights and freedoms do not override the identified legitimate interest? IFN must consider the nature of the various interests, the impact of the processing on individuals and on IFN, as well as the safeguards that IFN will put in place to reduce the risk to individuals.

IFN must always document the assessment it has carried out when considering the legitimate interest basis.

Data Privacy Impact Assessments (DPIA)

The Rule: Where the collection and use of personal data is likely to result in significant risks for the rights and freedoms of individuals, IFN must carry out an assessment into the impact of the proposed collection and use on individuals

Understanding the Rule

Where IFN intends to use personal data in a more 'intrusive' way it must carry out an initial assessment to consider whether the use is justified. Carrying out a DPIA helps to identify and minimise the privacy risks associated with the use of personal data. IFN may be able to rely on one DPIA for multiple instances of similar processing. If it intends to collect and use personal data in a way that could result in discrimination, identity theft, fraud or financial loss, IFN should consider whether a full DPIA is needed.

As part of the DPIA, IFN must evaluate the origin, nature, particularity and severity of any risk to the privacy of individuals.

Practical Steps

The Executive Director will be informed of any potential need for a DPIA. Use and collection of personal data will not proceed until guidance from the Executive Director has been received on whether a DPIA is required or not. The Executive Director will work with you to mitigate any potential risks to the privacy of individuals.

In certain circumstances, IFN may be required to consult with the Information Commissioner's Office (ICO) about the proposed use of personal data.

Ensuring data quality

The Rule: We must keep personal data accurate and up to date

Understanding the Rule

Processing inaccurate information can be harmful to individuals and to IFN. The main way of ensuring that personal data is kept accurate and up to date is by ensuring that the sources used to obtain personal data are reliable.

Individuals should be actively encouraged to inform us when their personal data changes.

Practical Steps

In the employment context, employees should be actively encouraged to update their details (e.g. change of address).

To ensure that personal data is accurate, it should generally be collected directly from individuals affected. All service users should be actively encouraged to update their contact details by inviting them, when communication occurs, to notify us of any changes in their personal data.

Retaining and disposing of data

The Rule: IFN must keep personal data only for as long as is necessary for a specific business purpose and ensure it is securely disposed of

Understanding the Rule

Personal data must only be kept where there is a business or legal need to do so. When IFN disposes of personal data, this must be done securely.

Laws, regulations or contractual obligations may require that certain personal data be kept for a specified length of time, and it may also be prudent to keep certain personal data for a specific period so that IFN is able to defend properly any legal claims or manage an ongoing relationship.

Documents (including paper and electronic versions and email) containing personal data must not be kept indefinitely (unless we have a clear purpose for doing so and a strong justification) and must always be securely deleted and destroyed once they have become obsolete or when that personal data is no longer required. Personal data must not be retained simply on the basis that it might come in useful one day without any clear view of when or why.

Practical Steps

IFN will follow all internal data retention policies in relation to:

- The key applicable retention requirements from both a business and (where applicable) legal perspective (for example, we keep application forms for Executive Director posts for 6 years, and application forms for Assistant Director posts for 1 year, and all other posts 12 months).
- Procedures for ensuring that personal data is properly retained and securely destroyed
- The process for suspending the destruction of documents in situations relating to pending, threatened or reasonably likely litigation, regulatory or governmental investigations
- The responsibilities of those involved in retention activities relating to personal data.

Honouring individuals' rights

The Rule: IFN must always be receptive to any queries, requests or complaints made by individuals in connection with their personal data and comply with those requests within the timeframes specified in the UK GDPR.

Understanding the Rule

IFN will reply to queries and complaints, usually free of charge to the individual, within a reasonable time and to the extent reasonably possible. IFN considers that the most important of all data protection rights is the ability of individuals to access the personal data that it holds about them and to expect that it will be corrected if it is inaccurate.

Individuals are entitled by law to be supplied (on request) with a copy of their personal data (including both electronic and paper records). Individuals are also entitled:

(a) to know the logic involved in decisions made about them;

(b) to ask us to erase their personal data;

(c) to object to how we process their personal data;

(d) to ask us to rectify any inaccuracies in their personal data;

(e) to suspend processing pending solution of an underlying disagreement; or

(f) to have us transfer their personal data to another organisation in a structured, commonly used and machine-readable format (where we are holding that personal data electronically).

In some cases, these rights only apply in limited, specific circumstances. The Executive Director should be consulted if a staff member, volunteer or trustee thinks that an individual is seeking to exercise a privacy right – in most cases we must respond within one month, unless there is a compelling case not to in which case this can be extended by two further months.

Practical Steps

Where IFN receives a request from an individual exercising their legal right to access, object to or modify their personal data, it must follow the steps set out in the UK GDPR and as set out in any relevant internal policies and procedures.

If a valid request concerns a change in that individual's personal data, such information must be rectified or updated, if appropriate to do so.

Taking appropriate security measures

The Rule: IFN must always take appropriate technical and organisational security measures to protect personal data

Understanding the Rule

Personal data must be kept secure. Technical, organisational, physical and administrative security measures (both IT and non-IT related) are necessary to prevent the unauthorised or unlawful processing or disclosure of personal data, and the accidental loss, destruction of, or damage to personal data.

When considering what level of security is required in each particular case, a number of factors must be taken into account including:

- The state of technological development
- The cost of implementing any measures
- The harm that might result from a breach of security
- The nature of the information to be protected as special categories of data require greater security

If IFN fails to take appropriate security measures, it may suffer a data security breach and can then be required to notify the ICO and the individuals affected. If it fails to comply with these reporting requirements, it can receive a fine.

Practical Steps

IFN must monitor the level of security applied to personal data and take into account current standards and practices. In particular, it must observe the requirements set out in its Cyber Security Policy and its Policy on use of personal devices for carrying out IFN work.

Any data security breach or seeming or likely breach, must be immediately reported to the Executive Director so as to put IFN in a position to mitigate the potential consequences.

Adopting Privacy by Design

The Rule: IFN must adopt privacy by design and by default in all systems, databases, tools and features we build to collect and use personal data

Understanding the Rule

Taking account of the particular circumstances of the data collection and use, the cost of implementing measures and risks to individuals, IFN must implement measures (such as pseudonymisation) that reflect data protection principles when it designs systems, databases, tools and features to process personal data.

Practical Steps

IFN must ensure that any privacy settings are by default set to the most privacy protective setting. It must ensure that the minimal amount of personal data is collected and used through its technology.

As far as technologically possible and as is proportionate (including taking account of associated costs) it should employ pseudonymised datasets to reduce risk to individuals' privacy.

Using subcontractors/suppliers

The Rule: IFN must ensure that providers of services to us also adopt appropriate and equivalent security measures

Understanding the Rule

Under the UK GDPR, where a provider of a service has access to IFN's personal data (e.g. as a payroll provider) IFN must impose strict contractual obligations dealing with the purposes and ways its personal data may be used and the data security of that information. This includes suppliers who host data on IFN's behalf.

Practical Steps

IFN must always carry out appropriate and proportionate due diligence which considers the supplier's security measures for processing personal data before it engages a supplier.

IFN must always enter into a written contract with any supplier that deals with personal data on its behalf. All contracts with suppliers should include standard contractual provisions designed to comply with the requirements of the UK GDPR.

Disclosing to third parties

The Rule: IFN must only disclose personal data to third parties where it has the consent of the individual, where required by law or where the third party is a supplier that has a need to know the information to perform its services and has entered into a contract with us containing the appropriate data privacy and security provisions

Understanding the Rule

At times, IFN may disclose personal data to suppliers, contractors, service providers and other selected third parties.

Prior to disclosing personal data to these parties, IFN will take reasonable steps to ensure that: (i) the disclosure of personal data is consistent with its Cyber Security Policy; (ii) the recipient of such information is identified; and (iii) where appropriate or required by law, the third party is contractually committed to complying with this Policy and/or IFN's instructions concerning the use of personal data as well as implementing appropriate security measures

to protect personal data, limiting further use of personal data, and complying with applicable laws.

In certain circumstances, IFN may be required to disclose personal data to third parties when required by law, when necessary to protect its legal rights, or in an emergency situation where the health or security of an individual is endangered. Prior to such disclosures, IFN must take steps to confirm that the personal data is disclosed only to authorized parties and that the disclosure is in accordance with this Policy, other applicable IFN policies and/or operating procedures, and applicable law.

Practical Steps

If a request is received from a third party asking for disclosure of personal data to them, the Executive Director should be consulted unless it is a business as usual request i.e. it is the type of request that you typically receive in connection with your role which you regularly comply with and involves no significant disclosure of personal data.

Legitimising international transfers

The Rule: International transfers of personal data are subject to certain legal restrictions and therefore IFN must ensure that all transfers are subject to appropriate protection

Understanding the Rule

Data protection law restricts international transfers of personal data to countries that do not ensure an 'adequate' level of data protection, and requires that appropriate safeguards are put in place.

The first question should always be whether the rules on international data transfers are triggered. Where we are involved in transferring personal data from the UK to a country outside the UK, we must comply with the rules on transfers of personal data.

The next question is whether there is an applicable 'adequacy' decision in place. All data transfers from the UK to a country in the EU or the EEA are considered adequate and no further steps are required. The European Commission maintains a list of other countries which provide adequate protection, which can be found here. The UK also adopts these adequacy decisions. There is no adequacy decision for the US.

If there is no applicable adequacy decision, then we need to consider appropriate safeguards[1]. Such safeguards can be achieved through a number of mechanisms such as contracts or internal policies. International transfers of personal data to countries that are not adequate are not allowed without appropriate steps being taken, such as contractual clauses which will protect the personal data that is being transferred. The UK's International Data Transfer Agreement ("**IDTA**") is a set of standard provisions approved by the UK Government. This is a complex area so please consult with the Executive Director if unsure. The UK IDTA applies to international data transfers from the UK to a country outside the UK (introduced by the UK Government in March 2022). The European Commission has also issued a set of Standard Contractual Clauses that apply to international data transfers from the EU to a country outside the EU.

[1] NB. The US Privacy Shield is no longer available.

1.1.1 We are also required to carry out 'transfer risk assessments' in respect of any international transfer of personal data to countries that are not adequate, taking into account the data protection law and practices of those countries, including the ability of public authorities in those countries to access personal data. Depending on the results of this assessment, we may need to implement further measures to ensure that the personal data is adequately protected after it's transferred.

If no appropriate safeguards are applicable, then we can consider certain derogations under UK data protection law. However, these should only ever be used as a last resort for one-off transfers.

Practical Steps

This Policy is a vital part of ensuring that we comply with our data protection obligations.

- You must not transfer any personal data outside of IFN across borders without checking whether a legal restriction is in place.
- If there is a legal restriction in place, we must consider how the personal data being transferred will be adequately protected (for example, through entering into the UK IDTA).
- We should also carry out Transfer Risk Assessments when transferring personal information from the UK to other countries which have not been declared 'adequate' under UK law.

Special categories of data

The Rule: IFN must only use special categories of data if it is absolutely necessary and, in most circumstances, it should obtain explicit consent from individuals to use their special categories of data.

Understanding the Rule

Special categories of data is information revealing an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, processing of genetic data or biometric data (for the purpose of uniquely identifying an individual), health and sex life or sexual orientation. Since this information is more intrusive, we must only use it where absolutely necessary and usually with the explicit consent of the individual affected.

The proposed collection and use of special categories of data should be scrutinized and challenged before proceeding. Consent from individuals to IFN's use of their special categories of data must be genuine and freely given.

IFN can only hold and make available special categories of data on an individual without their explicit consent if it has another lawful basis under applicable law. This may be the case, for example, where IFN holds information about an employee's health where this is necessary to exercise any obligation conferred by law on it in connection with employment.

Practical Steps

- IFN will always assess whether special categories of data are essential for the proposed use – why do we need it?

- IFN will only collect special categories of data when it is absolutely necessary in the context of our organisation – why do we need it?

- Application (or other) forms used to collect special categories of data must include suitable and explicit wording expressing the individual's consent.

- Consent must be demonstrable. Therefore, when it is collected verbally it must be recorded in such a form as to prove that the requisite information was provided to the individual and their response was able to be verified.

- Where consent is not relied upon, IFN must take steps to ensure that there is another lawful basis under applicable law for the collection and use of such information.

- The Executive Director should be informed of any planned significant use of special categories of data to verify the legitimacy of such use. The Executive Director is entitled to ask further questions and will work with staff, volunteers or trustees to mitigate any potential risks in this regard.

Collecting children's data

The Rule: IFN should only collect personal data of children when strictly necessary and, if it is relying on consent as the lawful basis, IFN may need to obtain verifiable parental consent.

1.1.1 *Understanding the Rule*

Children merit additional protection under data protection law. In particular around sending marketing to children or profiling children. IFN should not collect and use children's personal data to make automated decisions about them which have a legal effect or significantly affects a child.

Any privacy notice IFN provides to children must be specifically tailored to them.

If we offer an online service directly to children or which could be used by children and we rely on consent as the lawful basis, only children aged 13 or over can provide valid consent. Otherwise, we need to obtain verifiable parental consent. We are required to make reasonable efforts to verify that the person giving consent is the parent/guardian.

Practical Steps

- IFN will always assess whether it really needs to collect children's data.

- IFN will consider how it will identify the age of a child.

- IFN will ensure any privacy notices provided to children are age appropriate.

- IFN will identify if it is relying on consent as the lawful ground where providing an online service and whether the online service could be used by children.

- IFN will use an appropriate verification tool if it needs to obtain verifiable parental consent.

Legitimising direct marketing

The Rule: IFN must obtain consent from individuals to use their details for direct marketing where the law requires and always allow them to opt out.

Understanding the Rule

In the context of electronic marketing (e.g. by email or SMS), the default position is that IFN must obtain prior consent from individuals before sending marketing to them.

One of the key data protection rights is that individuals have the right to object to the use of their personal data for direct marketing purposes and we must always notify individuals of their right.

Practical Steps

IFN will ensure we collect valid consent from individuals before sending them e-marketing if consent is required by law.

IFN will ensure that the privacy notice made available when personal data is collected includes the relevant opt-out mechanisms regarding marketing communications.

Honouring opt-outs

The Rule: IFN must always suppress from marketing initiatives the personal data of individuals who have opted-out of receiving marketing information.

Understanding the Rule

It is essential that individuals' choices are accurately identified when direct marketing campaigns are carried out. A failure to comply with an individual's opt-out choice (e.g. by sending a mailing to an individual who has previously indicated to us that he or she does not wish to receive mailings) is likely to lead to complaints from the individual and possible scrutiny or enforcement action being taken by the ICO.

Practical Steps

Where IFN is responsible for a direct marketing campaign about IFN and it is using information collected by IFN, it must take all necessary steps to prevent the sending of marketing materials to individuals who have opted-out.

4. COMPLYING WITH THE RULES

Why is compliance with the Rules important?

It is important that all staff, volunteers and trustees comply with the Rules since all are responsible. A failure to comply could expose IFN to regulatory and/or legal action which could mean the payment of compensation, damages and/or fines as well as other remedies.

What happens if someone breaches a Rule?

If a staff member, volunteer or trustee breaches a Rule, even inadvertently, they must immediately inform the Executive Director even if they are not certain whether the breach is serious. They should always voluntarily tell the Executive Director of any serious breaches since any deliberate cover up or attempts to mislead about a breach will be taken as a serious disciplinary matter.

While IFN would always seek to work through any breach incident in order for the relevant individual to understand the ramifications of their actions or omissions and continue to work on the same basis, regrettably, in some circumstances, IFN may have to commence disciplinary action against the person if the breach is of a particularly damaging nature and, ultimately, IFN may have to terminate that person's contract where appropriate.

Additionally staff members, volunteers and trustees should be aware that knowingly or recklessly obtaining or disclosing personal data may be a criminal offence and could also result in damages or compensation claims against them.

Monitoring compliance with the Rules

IFN will periodically monitor and check that it is complying with these Rules. All employees, volunteers and trustees must co-operate when asked to do so with any such checks and any outcomes, including remediation plans.

Are there exceptions to compliance with the Rules?

In limited circumstances, such as co-operating in criminal or other government investigations or inquiries, it may be appropriate for IFN to rely on an exemption from compliance with part or all of these Rules. All such exception requests must be approved by the Executive Director, who may take further legal advice as appropriate.

Who enforces data protection law?

Data protection law is usually enforced by data protection regulators and the courts. In the UK, the data protection regulator is the ICO with powers to serve notices on us and to conduct assessments of our operations and to issue fines.

5. TRAINING ON THE RULES

We require all relevant employees and contractors to receive training on the Rules. This includes induction training and refresher training every two years through Virtual College.

6. IMPLEMENTATION

This Policy is effective from 12 February 2019.

7. MAINTENANCE AND CONTACT

The review and maintenance of this Policy is the responsibility of the Board. Minor updates and corrections may be made by the staff and notified to the Finance and General Purposes Subcommittee, but any changes to substance must be agreed by the Board.

This policy will be reviewed every 2 years, or sooner where necessary.

April 2022

[Version 1.1]

Declaration

I confirm I have read and understood The Inter Faith Network for the UK's Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a

- ☐ *Member of staff*
- ☐ *Volunteer*
- ☐ *Trustee/ management committee member*

Signature:

Print name:

Date:

Date of undertaking training:

Please return this form to Dr Harriet Crabtree, Executive Director