Data Protection Policy

The Duke of Edinburgh's International Award Foundation

September 2019
Version 1.0

Version control

Version	Date	Author	Notes
1.0	January 2019	Director of Information Technology -YS	

Relevant policies

1. The National Award Operator Licence
2. Operating Partner Licence
3. Serious Incidence Reporting Policy
4. Safeguarding Policy
5. Award Community Guidelines

Contents

INDEX

1. INTRODUCTION

1.1 The Duke of Edinburgh's International Award Foundation (the "**Foundation**") is responsible for the prestigious Duke of Edinburgh's Award (the "**Award**"). The Foundation coordinates the Award through a number of different organisations, including:

Intaward Limited (the commercial subsidiary of the Foundation);

A network of Award Operators, including:

(i) National Award Operators ("**NAOs**"); and

(ii) Independent Award Centres ("**IACs**")

(iii) Wholly Owned Foreign Enterprise {WOFE] (specific to China)

For the purposes of this Policy, we refer to the above organisations (including the Foundation) as the "**Association**" (with each individual organisation an "**Operator**").

1.2 The Foundation makes available to the Association digital / online tools to assist in the delivery of the Award, including, but not limited to:

a. the Online Record Book (or "**ORB**")

b. the Online Learning Hub (or "**OLH**")

c. Award Communities

d. the Extranet (this will supersede Award Communities and the Online Learning Hub)

e. Salesforce (*CRM*)

f. QuickPay (secure Payment Card processing)

g. EventPowWow (bookings for Events and Training)

This means that much of the personal data relating to the Award is held by the Foundation, but accessible by Association around the world.

1.3 The Foundation has a responsibility to ensure that it uses personal data in accordance with the law. As such, the Foundation has developed this Data Protection Policy ("**Policy**"). Everyone in the Foundation is accountable for upholding the Policy's requirements, and the Foundation requires employees and volunteers of each Operator to follow this Policy, as well.

1.4 As the Award is delivered around the world, the Foundation is committed to handling personal data responsibly and in compliance with applicable data protection laws worldwide. This Policy is designed to provide a global baseline with respect to the protection of personal data, based

upon European Union data protection standards. The Foundation recognises that in some jurisdictions certain laws may impose additional requirements. The Foundation or the relevant Operator will handle personal data in accordance with all such applicable laws.

1.5 This Policy covers use of personal data about those categories of individual identified in section 2.5 below. We need to comply with the rules set out in this Policy about how we use personal data. No one is exempt from compliance with these rules.

1.6 This Policy does not form part of any employee or volunteer contract, nor does it form part of any contract between the Foundation and an Operator, and so it may be amended at any time. You will be notified of any significant changes.

YOU ARE REQUIRED TO FAMILIARISE YOUSELF WITH THIS POLICY.

2. BACKGROUND

2.1 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.

Personal data is interpreted broadly by European data protection authorities and courts. Information may be personal data even if a person's name is not associated with it.

All organisations established in the countries of the European Union and in the UK must meet the requirements set out in the General Data Protection Regulation (**GDPR**).

2.2 What are we doing about it?

The Foundation treats compliance with its obligations very seriously. We wish to maintain the highest possible standards of compliance to ensure in particular that individuals are properly protected and that our internal procedures are designed to ensure compliance. 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.

In order to help make sure this Policy is understood and adhered to, each Operator must appoint a senior representative to be in charge of data privacy compliance, a "**Data Privacy Lead**". It is the responsibility of the Data Privacy Lead to ensure the relevant Operator's compliance with this Policy, and any applicable data protection legislation.

Each National Award Operator must make the name and contact details for its Data Privacy Lead available to its staff and volunteers, as well as to the Foundation.

At present, it is not necessary for Independent Award Centres to have a nominated Data Privacy Lead.

The Data Privacy Lead for the Foundation (and Intaward Limited) is: **Yogesh Sharma, Director of IT** (Yogesh.Sharma@intaward.org).

2.3 What are the consequences if we get it wrong?

Getting it wrong is serious. It could also lead to complaints from individuals, compensation claims, fines from regulators and bad publicity for the Foundation and Award. Because of the seriousness of the consequences, if you deliberately fail to observe this Policy we will consider disciplinary action against you.

2.4 Why is this Policy important?

It is vital that those working as part of the Award observe this Policy because the collection and use of personal data is part of our everyday business. We must ensure that we use the information we hold about individuals in accordance with the law.

2.5 What types of personal data does the Foundation collect?

The Foundation collects personal data regarding:

- *Applicants, employees, volunteers and contractors of the Foundation and the Association. Board of Trustees*
- *Award Participants*
- *Parents / Guardians of Award Participants Award Leaders*
- *Supporters*
- *Donors*
- *Individuals at partner organisations*
- *Supplier personnel*

2.6 When should you collect and use personal data?

You must only collect and use personal data in compliance with this Policy and the Rules set out below.

2.7 How does this Policy relate to other policies within the Foundation?

This Policy sits alongside the Foundation's *internal* Information / IT Security Policy and Operator License Agreements.

2.8 Want more information?

If you want more information about data protection and how the rules affect the Foundation and/or your Operator please contact your relevant Data Privacy Lead.

3. THE RULES

3.1 Ensuring Transparency

The Rule: We must be transparent about the personal data that we hold on individuals. This includes describing the purposes for which we use personal data.

3.1.1 Understanding the Rule

Being transparent in the way we use and share personal data is an important step to demonstrate good data protection practices. Transparency is also a core principle of EU data protection law. As an example, the GDPR requires us to tell individuals (such as Award Participants) when and how we use their personal data.

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

3.1.2 Practical Steps

The individuals whose personal data we collect and use must be provided with information about fair processing. For example, suitable wording is included in our privacy notices provided to individuals who use the ORB, Online Learning Hub, Award Communities and those who visit our main website.

If we offer 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 must be clear, conspicuous and easy to use.

3.2 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 organisational purpose. These purposes must be lawful and justifiable.

3.2.1 Understanding the Rule

We must only collect and use personal data where (i) it is relevant to our legitimate organisational purposes (e.g. a HR purpose or to administer a specific award), (ii) we can rely on a lawful basis (or bases – see paragraph 3.2.2 below), (iii) the purposes are identified in the privacy notice which has been provided to individuals, and (iv) the collection and use is within the individual's expectations (which a privacy notice can help to shape).

3.2.1 Understanding the Rule

We must only collect and use personal data where (i) it is relevant to our legitimate organisational purposes (e.g. a HR purpose or to administer a specific award), (ii) we can rely on a lawful basis (or bases – see paragraph 3.2.2 below), (iii) the purposes are identified in the privacy notice which has been provided to individuals, and (iv) the collection and use is within the individual's expectations (which a privacy notice can help to shape).

3.2.2 Practical Steps

When collecting personal data from individuals, we must ensure that the privacy notice made available to those individuals identifies all of the purposes for which the personal data may be used. If you do not believe your Operator's privacy notice covers the points discussed above, please check with your Data Privacy Lead.

We 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 which has been communicated to the individual. Personal data that is not necessary for any legitimate organisational purpose should not be collected or accessed. You must not use any personal data accessed through your role for any private interest.

Two of the key lawful bases are consent and legitimate interests – these are explained in more detail in the box below. The others are (in summary):

- where use of personal data is necessary in order to perform a **contract** to which the relevant individual is a party, or to take steps at the request of that individual prior to entering into a contract;
- where it is necessary to use the personal data to comply with a **legal obligation**; and
- where it is necessary to use the personal data to protect the "**vital interests**" of the relevant individual (please note this is generally restricted to life or death emergencies).

Can we rely on consent?

In some circumstances (though not always), use of personal data requires us to obtain the relevant 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 we must provide clear and unambiguous information on the purposes the personal data will be used for when we collect consent. Consent must also be genuine and 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 we obtain documented evidence of the declaration of consent (e.g. in writing or via the use of an opt-in online). Our use of personal data must not fall outside 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 – we 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 effectively 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 to that proposal, either orally or in writing (which could be a wet ink signature on a piece of paper, or electronically through the use of of an electronic 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?

European data protection law 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 we can rely on it. However, if we wish to rely on the legitimate interest lawful basis we need 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: administering awards, 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 we further the same interest without processing personal data, or could another less intrusive way be used?

3. Balance the identified interest with the rights and freedoms of individuals whose personal data we will process. Are we sure that the rights and freedoms of individuals do not override the identified legitimate interest? In considering how to balance the different factors we must consider the nature of the various interests, the impact of the processing on individuals and on us (including how intrusive it is), as well as the safeguards that we will put in place to reduce any risk to individuals.

We should document the assessment we have carried out when considering the legitimate interest basis

3.3 Data Protection Impact Assessments

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

3.3.1 Understanding the Rule

Where we intend to use personal data in a more intrusive way, we must carry out an initial assessment to consider whether the use is justified. Carrying out a DPIA (Data Protection Impact Assessment) helps us identify and minimise the privacy risks associated with the use of personal data. We may be able to rely on one DPIA for multiple instances of similar processing. Additionally, if we intend to collect and use personal data in a way that could result in discrimination, identity theft, fraud or financial loss, we must consider whether a DPIA is needed.

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

3.3.2 Practical Steps

The Foundation's Data Privacy Lead should be informed whenever you have identified a potential need for a DPIA. You must not proceed with the collection and use of personal data until you have received guidance from your Data Privacy Lead on whether a DPIA is required or not. Your Data Privacy Lead (and the Foundation's Data Privacy Lead, if appropriate) will work with you to mitigate any potential risks to the privacy of individuals.

In certain circumstances (such as where the DPIA identifies high risk which we cannot mitigate through safeguards), we may be required to consult with the Information Commissioner's Office (**ICO**) or relevant local data protection authority. Please notify the Foundation's Data Privacy Lead, if you think this may apply.

3.4 Ensuring data quality

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

3.4.1 Understanding the Rule

Processing inaccurate information can be harmful to individuals and the Foundation. The main way of ensuring that personal data is kept accurate and up to date is by ensuring that the sources we use to obtain personal data are reliable.
Individuals should be actively encouraged to inform us when their personal data changes.

3.4.2 Practical Steps

In the employment context, employees should be actively encouraged to update their details (e.g. change of address) and HR should also perform routine updates. This also applies to Award Participants, as they should be encouraged to update their details on the ORB.

To practically ensure that personal data is accurate, it should generally be collected directly from individuals affected. For example, users of resources such as the ORB and Online Learning Hub should be actively encouraged to update their details by inviting them, when communication occurs, to notify us of any changes in their personal data.

When an individual disputes the accuracy of personal data that we hold about them, we are not required to amend the personal data if we consider we can justify the original recording of the personal data. However, we should include a supplementary statement on the record to indicate their disagreement on accuracy.

3.5 Retaining and disposing of data

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

3.5.1 Understanding the Rule

Any personal data must only be kept where there is an organisational or legal need to do so. When we dispose of personal data, this must be done in a secure manner.

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

Documents (including paper and electronic versions and email) containing personal data must not be kept indefinitely 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.

3.5.2 Practical Steps

We must follow all internal data retention policies in relation to:

The key applicable retention requirements from both an organisational and (where applicable) legal perspective.

Procedures for ensuring that personal data is properly retained when needed and securely destroyed afterwards.

The process for suspending the destruction of documents in situations relating to pending, threatened or reasonably likely litigation, regulatory or governmental investigation.

The responsibilities of those involved in retention activities relating to personal data

3.6 Honouring individuals' rights

The Rule: We must always be receptive to any queries, requests or complaints made by individuals in connection with their personal data and ensure they are responded to promptly, and no longer than two working weeks from receiving

3.6.1 Understanding the Rule

In certain circumstances we have a legal obligation to reply to queries and complaints within a reasonable time and to the extent reasonably possible concerning the processing of personal data by us. We consider that the most important of all data protection rights is the ability of individuals to **access** the personal data that we hold about them and to expect that it will be corrected if it is inaccurate.

Individuals are entitled under EU data protection law (on request) to be supplied with a copy of any personal data held about them (including both electronic and paper records). Individuals are also entitled to know the logic involved in decisions made about them.

An individual also has the right to seek erasure of their data and to request portability of their data (i.e. that we provide their data to them in a structured, commonly used and machine-readable format), as well as object to our use of their personal data and seek restriction of our use.

3.6.2 Practical Steps

Where we receive a request from an individual exercising their legal right to access, object to or modify their personal data, we must follow defined procedures to ensure that valid requests are processed in line with applicable legislation.

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.

3.7 Taking appropriate security measures

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

3.7.1 Understanding the Rule

Personal data must be kept secure. Technical, organisational, physical and administrative security measures (both computer system and non-computer system related steps) 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 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

In certain circumstances, where we fail to take appropriate security measures, we may suffer a data security breach and can then be required to notify the data protection authority and affected individuals.

3.7.2 Practical Steps

We must monitor the level of security applied to personal data and take into account current standards and practices. In particular, we must observe the requirements set out in the Foundation's Information / IT Security Policy and any other requirements set out under the applicable local data protection laws.

If you become suspicious or are actually aware of any data security breach, you must immediately report the breach to the Data Privacy Lead (where one has been nominated) for your National Award Operator
(NAO) or your National Director. In the case of Independent Award Centres (IACs) please advise your Regional Operations Manager, as well as the Data Privacy Lead for the Foundation. When we become aware of a breach, we can take protective measures that can effectively mitigate the consequences of the breach.

In general, we must respond to any breach with a documented plan, which explains how we became aware of the breach, how we immediately contained it, whether we are obliged to notify the ICO or relevant local data protection authority, and/or affected individuals and what we will do to prevent it happening in the future.

3.8 Adopting Privacy by Design

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

3.8.1 Understanding the Rule

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

3.8.2 Practical Steps

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

As far as technologically possible, and proportionate (including taking account of the cost of implementation) we should employ pseudonymised datasets to reduce risk to individuals' privacy.

3.9 Using subcontractors/suppliers

The Rule: We must ensure that providers of services to us also adopt appropriate and equivalent security measures in relation to any personal data they process on the Foundation's or Operator's behalf.

3.9.1 Understanding the Rule

Under EU data protection law, where a service provider has access to our personal data (e.g. as a payroll provider) we must impose strict contractual obligations dealing with the purposes and ways the personal data may be used and ensuring appropriate security of that personal data. This includes suppliers who host personal data on our behalf.

3.9.2 Practical Steps

We must always carry out appropriate due diligence which considers the supplier's security measures for processing personal data before we engage such a supplier.

We must always enter into a written contract with any supplier that deals with personal data on our behalf. All contracts with such suppliers should include standard contractual provisions. Consult with the Data Privacy Lead for your Operator to ensure contracts are up to date with the most recent data protection provisions. The Data Privacy Lead should escalate a contract to the Data

Privacy Lead for the Foundation if they are uncertain about the approach for a particular service provider.

3.10 Disclosing to third parties

The Rule: We must generally only disclose personal data to third parties where we have the consent of the individual, where required by law or where the third party is a subcontractor/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 protection and security

3.10.1 Understanding the Rule

At times, we may disclose personal data to suppliers, contractors, service providers and other selected third parties (including disclosures between the Foundation and Association).

Prior to disclosing personal data to these parties, we need to take reasonable steps to ensure that: (i) the disclosure of personal data is consistent with our *internal* Information / IT 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 our 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, we may be required to disclose personal data to third parties when required by law, when necessary to protect our legal rights, or in an emergency situation where the health or security of an individual is endangered. Prior to such disclosures, we 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 policies and/or operating procedures, and applicable law.

3.10.2 Practical Steps

If you receive a request from a third party asking you to disclose personal data to them, you should contact your Data Privacy Lead 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. For example, providing the contact details for the Foundation or an Operator.

Any disclosures must be in accordance with the Foundation's internal policies and procedures.

3.11 Legitimising international transfers

The Rule: International transfers of personal data are subject to certain legal restrictions and therefore we must ensure that all transfers are subject to appropriate protection, such as through putting specific contracts in place.

3.11.1 Understanding the Rule

EU data protection law restricts transfers of personal data to countries that do not ensure an 'adequate' level of data protection. There is then a requirement to implement appropriate safeguards. Appropriate safeguards can be achieved through a number of mechanisms – usually a contract containing European Commission-approved clauses. International transfers of personal data outside the Foundation are not allowed without appropriate steps being taken. For example, this is one of the reasons why the Foundation has put in place data sharing agreements with the Award Operators.

3.11.2 Practical Steps

We must not transfer any personal data across borders without checking whether a legal restriction is in place (either under EU or local applicable data protection law). This includes if you are dealing with service providers or third parties based in another country and we are transferring personal data to them or allowing
them to remotely access our systems/data. When in doubt about the lawfulness of any transfer, please contact your Data Privacy Lead on how to proceed.

3.12 Safeguarding the use of special categories of data

The Rule: We must only use special categories of data if it is absolutely necessary for us to use it and we must be able to rely on an additional lawful basis (or exception).

3.12.1 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. Data about actual or alleged criminal offences, whilst not special category data, is similarly afforded greater protection under the law.

Since this information is more intrusive, we must only use it where absolutely necessary.

The proposed collection and use of special categories of data should be heavily scrutinized before proceeding. The explicit consent from individuals to our use of their special categories of data must be genuine and freely given.

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

Therefore, when adding questions to application forms and other forms that will capture personal data, consider carefully whether special categories of data are being collected, whether these are

proportionate and necessary, and whether we need to obtain explicit consent (including by making clear these questions are optional).

3.12.2 Practical Steps

- We must always assess whether special categories of data are essential for the proposed use – why do we need it?
- We must 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 could be verified.
- Where consent is not relied upon, we must take steps to ensure that there is another lawful basis under applicable law for the collection and use of such information.
- Your Data Privacy Lead (where you have appointed one) or your National Director, as well as the Data Privacy Lead for the Foundation, should be informed of any planned significant use of special categories of data to verify the legitimacy of such use. Your Data Privacy Lead (and the Data Privacy Lead from the Foundation, as appropriate) will work with you to mitigate any potential risks. In certain circumstances, we may be required to consult with the local data protection authority about the proposed use of such special categories of data.

3.13 Collecting children's data

The Rule: We should only collect children's personal data when strictly necessary and, if we are relying on consent as the lawful basis, we may need to obtain verifiable parental consent.

3.13.1 Understanding the Rule

Children merit additional protection under data protection law. In particular, there are greater risks around sending marketing to children or profiling children. We 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 we provide to children should be specifically tailored to them (for example, the privacy notice for the ORB).

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, in the UK only children aged 13 or over can provide valid consent. Other countries may have a different age limit for when a child can give valid consent. If we cannot obtain

valid consent from a child, 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.

3.13.2 Practical Steps

- We must always assess whether we really need to collect children's

  data. We must consider how we will identify the age of a child.

- We must ensure any privacy notices provided to children are age appropriate.
- We must identify if we are relying on consent as the lawful ground where providing an online service and whether the online service could be used by children.
- We must use an appropriate verification tool if we need to obtain verifiable parental consent

3.14 Legitimising Direct Marketing

The Rule: We must obtain consent from individuals to use their details for direct marketing where the law requires. We must always allow individuals to opt out of receiving marketing information.

3.14.1 Understanding the Rule

For electronic marketing (e.g. by email or SMS), the default position is that we must obtain consent from individuals before sending marketing to them.

'Marketing' is interpreted very widely by regulators, and effectively means any marketing, advertising or promotional material, including fundraising. The marketing content does not need to be the sole or main content of the relevant material for the consent requirement to apply.

Individuals have the right to object to the use of their personal data for direct marketing purposes and we must always notify individuals of this right.

In some cases there may be exemptions from this general requirement to obtain consent, for example where such material is sent to a business email address. Please speak to your Data Privacy Lead if you have any questions.

3.14.2 Practical Steps

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

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

3.15 Honouring Opt-outs

The Rule: We must always suppress from marketing initiatives the personal data of individuals

3.15.1 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 or other relevant data protection authorities.

3.15.2 Practical Steps

Where we are responsible for a direct marketing campaign about the Award, we must take all necessary steps to prevent the sending of marketing materials to individuals who have opted-out.

4. COMPLYING WITH THE RULES

4.1 Why is it important that I comply with the Rules?

It is important that everyone complies with the Rules. A failure to comply with the Rules could expose us to regulatory and/or legal action which could mean the payment of compensation, damages and/or fines as well as other remedies.

4.2 What happens if I breach a Rule?

If you breach a Rule, even inadvertently, you must immediately inform your Data Privacy Lead even if you are not certain whether the breach is serious. We will consider any deliberate cover up or attempts to mislead us about a breach as a serious disciplinary matter.

While we would always seek to work through any breach incident with you in order for you to understand the consequences of your actions and continue to work on the same basis, regrettably, in some cases, we may have to commence disciplinary action against you if the breach is of a particularly damaging nature and, ultimately, we may have to terminate your contract.

Additionally you should note that knowingly or recklessly obtaining or disclosing personal data may be a criminal offence and could also result in damages or compensation claims against you.

4.3 Auditing compliance with the Rules

We will conduct periodic audits to ensure compliance with the Rules. All employees and contractors (including those at each NAO or IAC, as well as within the Foundation) must participate with such audits and any outcomes, including remediation plans.

Reviews for NAOs and IACs will normally be carried-out as part of the Foundation's regular License Review process.

4.4 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 to rely on an exception from compliance with part or all of these Rules. All such exception requests must be approved by your Data Privacy Lead and the Data Privacy Lead for the Foundation should be notified.

4.5 Who enforces data protection law?

Data protection law is usually enforced by data protection regulators and the courts. In the UK, the regulator is the ICO. It has powers to serve notices on us, investigate our operations and, ultimately and for serious breaches, to issue fines.

5. TRAINING ON THE RULES

We require all relevant employees and contractors to receive training on the Rules.

Each Operator is responsible for providing its own training. The Foundation will provide overall training via: the Data Protection Online Learning Hub modules.

Further information and training will be available with the Foundation's Online Learning Hub

6. IMPLEMENTATION

This Policy is effective from **01 September 2019**

7. MAINTENANCE AND CONTACT

The review and maintenance of this Policy is the responsibility of the Foundation's Data Privacy Lead. Queries and feedback should be directed to the Foundation's Data Privacy Lead: **Yogesh Sharma, Director of IT** (Yogesh.Sharma@intaward.org)**.**