Data Protection Policy

The Duke of Edinburgh's International Award Foundation

September 2023
Version: 2.0

Version control

Version	Date	Author	Notes
1.0	January 2019	Yogesh Sharma – Director of Information Technology	
2.0	September 2023	Kelly Cox & Peter Orrey – Data Privacy Leads.	Update to Data Privacy Lead information and formatting.

Relevant policies

1. The National Award Operator Licence
2. The Operating Partner Licence
3. Serious Incident Reporting Policy
4. Safeguarding Policy
5. Data Privacy Notice
6. Award Community Terms and Conditions
7. Online Record Book Terms and Conditions

Contents

1. Introduction

1.1 The Duke of Edinburgh's International Award Foundation (the "Foundation") is responsible for the 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 Operators, including:

(i) National Award Operators ("**NAOs**");
(ii) Operating Partners ("**OPs**"); and
(iii) Independent Award Centres ("**IACs**")

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 Award Community
c. Salesforce (CRM)
d. Facilities for Operators to make online payments to the Foundation
e. Alumni Platform

This means that much of the personal data relating to the Award is held by the Foundation, but accessible by the relevant Operator.

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 adhere to this Policy, as well as the international licence agreements.

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 UK General Data Protection Regulation (GDPR) 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.

1.6 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.

1.7 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**).

1.8 The Foundation has developed this Policy to ensure that the personal data we collect, and use is done so in accordance with applicable data protection laws.

1.9 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.

1.10 Each National Award Operator and Operating Partner must make the name and contact details for its Data Privacy Lead available to its staff and volunteers, as well as to the Foundation, as per the international licence agreements.

The Data Privacy Leads for the Foundation (and Intaward Limited) are **Kelly Cox, Licensing and Compliance Manager** (Kelly.Cox@intaward.org) and **Peter Orrey, Senior Digital Programmes Manager** (Peter.Orrey@intaward.org).

2. The Principles

2.1 All Data Protection processes and procedures carried out and upheld by the Foundation, and through the international licence agreements, are underpinned by the following seven key principles as per UK GDPR legislation. The table below outlines the principle, what this means and how this is implemented in practice.

2.2 When collecting, processing or retaining personal data all of the principles below should be considered and measures implemented to ensure the greatest level of protection is awarded to all data subjects.

Principle	What	How
Ensuring Transparency	We must be transparent about the personal data that we hold on individuals. This includes describing the purposes for which we use personal data.	✓ Clear Privacy Notices. ✓ Clear, conspicuous, and easy to use opportunities to opt-in, access, correct or remove/opt-out.
Purpose Limitation	We must only collect and use personal data for the purpose(s) communicated to the individual.	✓ Privacy Notices that explain all the ways personal data will be used and on what lawful basis.
Data Minimisation	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.	✓ Do not collect additional data outside of what is advised in Privacy Notices or what is needed for the task/action.
Accuracy	We must keep personal data accurate and up to date.	✓ All members of the Association should be encouraged to keep any personal data held up to date regularly – including employee information and participant information held on the Online Record Book (ORB). ✓ Collect personal data directly from the individuals affected.
Storage Limitation	We must keep personal data only for as long as is necessary for a specific organisational purpose and ensure it is securely disposed of.	✓ Only keep personal data where there is an organisational or legal need to and for a specified period of time. ✓ Follow all internal data retention policies which will include:

		- Retention requirements - Procedures for securely retaining and destroying data. - Processes for suspending destruction of data.
Integrity and Confidentiality	We must ensure that we have appropriate security measures in place to protect the personal data we hold.	✓ Follow all internal Information/IT Security Policy requirements. ✓ Report any breach, or suspected breach, of personal data to the relevant Data Privacy Lead or contact person. ✓ Respond to any breach with a documented plan.
Accountability	We must take responsibility for what we do with personal data and how we comply with the other principles. We must have appropriate measures and records in place to be able to demonstrate our compliance.	✓ Appointing Data Protection Officers/Leads to advise on compliance with the above principles. ✓ Keeping a store of processes and procedures for the management of all personal data.

3. Lawful Bases & Consent

3.1 When processing any form of personal data, the Foundation is required to ensure there is a lawful basis for doing so. The lawful bases according to UK GDPR legislation are as follows:

(i) Consent
(ii) Performance of a contract
(iii) Compliance with a legal obligation
(iv) Necessary to protect the vital interests of a person
(v) Necessary for a public task
(vi) Legitimate Interest

3.2 Two of the key lawful bases are consent and legitimate interests – these are explained in more detail 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**;
- where use of personal data is needed to perform a specific task in the public interest that is set out in law; 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).

3.3 In some circumstances 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 European data protection law allows processing of personal data where an organisation can rely on the **legitimate interest** lawful basis.

3.9 If we wish to rely on the legitimate interest lawful basis, we need to be able to identify a legitimate interest for using personal data for a particular purpose. A test then must be carried out to consider whether the processing of the personal data is necessary for satisfying that identified and balance the identified with the rights and freedoms of individuals whose personal data we are processing. The outcome of this test must be documented.

4. Adopting Privacy by Design

4.1 Privacy by design is a concept that privacy should be integrated into the design and development of all processes and procedures at the beginning. 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.

4.2 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.

4.3 Any privacy settings must be, 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.

4.4 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.

5. Third Parties and Sub-Contractors

5.1 Providers of services to the Foundation must also adopt appropriate and equivalent security measures in relation to any personal data they process on the Foundation's or Operator's behalf.

5.2 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.

5.3 All appropriate due diligence which considers the supplier's security measures for processing personal data must be completed before we engage such a supplier.

5.4 There must always be a written contract in place 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.

5.5 In most circumstances personal data should only be disclosed 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.

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

5.7 Prior to disclosing personal data to third parties reasonable steps must be taken 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.

5.8 In certain circumstances, there may be a requirement 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.

5.9 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.

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

6. International Transfers

6.1 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.

6.2 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.

6.3 Personal data must not be transferred 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.

7. Safeguarding and Special Category Data

7.1 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.

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

7.3 Special categories of data can only be held and made available without 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.

7.4 To ensure the necessary safeguards are in place for special category data it is a requirement to:

(i) Assess whether special categories of data are essential for the proposed use;
(ii) Only collect special categories of data when it is absolutely necessary in the context of our organisation;
(iii) Ensure application and other forms used to collect special categories of data include suitable and explicit wording expressing the individual's consent;
(iv) Make sure consent is 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;
(v) Where consent is not relied upon, steps must be taken to ensure that there is another lawful basis under applicable law for the collection and use of such information; and
(vi) 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.

7.5 Children merit additional protection under data protection law. UK GDPR defines a child as anyone under the age of 18, in accordance with the UN Convention on the Rights of the Child. 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.

7.6 Any privacy notice we provide to children should be specifically tailored to them (for example, the privacy notice for the ORB).

7.7 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.

7.8 To ensure the necessary safeguards are in place for children's data it is a requirement to:

(i) Assess whether we really need to collect children's data;
(ii) Consider how we identify the age of the child;
(iii) Ensure any privacy notices provided to children are age appropriate;
(iv) 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; and
(v) Use an appropriate verification tool to obtain verifiable parental consent.

8. Direct Marketing and Opt-Outs

8.1 Consent must be obtained from individuals to use their details for direct marketing where the law requires. Individuals must always have the option to opt out of receiving marketing information.

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

8.3 '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.

8.4 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.

8.5 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.

8.6 A privacy notice must be made available when personal data is collected and must include the relevant opt-out mechanisms regarding marketing communications.

8.7 Any personal data of individuals who have opted-out of receiving marketing information must always be suppressed from marketing initiatives.

8.8 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 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.

9. Data Protection Impact Assessments and Data Breaches

9.1 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.

9.2 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.

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

9.4 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.

9.5 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.

9.6 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 or your Operating Partner (OP) or Award Manager. 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.

9.7 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.

9.8 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.

10. Audits, Compliance and Training

10.1 Periodic audits will be carried out to ensure compliance with the Rules. All employees and contractors (including those at each NAO, OP or IAC, as well as within the Foundation) must participate with such audits and any outcomes, including remediation plans.

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

10.3 We require all relevant employees and contractors to receive training on Data Protection processes and procedures.

10.4 Each Operator is responsible for providing its own training.

11. Maintenance and Contact

11.1 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 Leads: Kelly Cox (Licensing and Compliance Manager) and Peter Orrey (Senior Digital Programmes Manager) at info@intaward.org

11.2 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.

11.3 This Policy may change from time to time – for example, to take into account changes at IAF or to reflect changes in regulation or legislation. It was last updated in September 2023.