



Policy Document

DATA PROTECTION POLICY

Policy Owner	The Duke of Edinburgh's International Award Nepal
Board Approval	December 1, 2024
Policy Responsibility	Data Protection Lead
Issue Date	December 4, 2024
Last Review	N/A

Version control

Version	Date	Author	Notes
1.0	1October 2024	Senior Operations and Programme Officer	Approved by the Executive Committee (Dec 1, 2024)

Relevant Policies:

Sub License Contract
Serious Incident Reporting Policy
Safeguarding Policy
Award Community Terms and Conditions
Online Record Book Terms and Conditions

CONTENTS

Introduction	3
Key Principles	3
Lawful Bases and Consent	4
Adopting Privacy By Design	5
Third Party Supplier	5
Safeguarding and Special Category Data	5
Data Protection Impact Assessment and Data Breaches	6
Audits, Compliance and Trainings	6
Maintenance and Contact	6

Introduction

Saskham Yuwa Nepal, is the National Award Operator (NAO) and administrative body of The Duke of Edinburgh's Award in Nepal. The NAO is sub-licensed by The Duke of Edinburgh's International Award Foundation (The Foundation), a charity responsible for The Duke of Edinburgh's Award.

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

- the Online Record Book (or "ORB")
- the Award Community
- Alumni Platform

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

The NAO has a responsibility to ensure that it uses personal data in accordance with the law. As such, the NAO has developed this Data Protection Policy ("Policy"). Everyone in the NAO is accountable for upholding the Policy's requirements, and the NAO requires employees and volunteers to adhere to this Policy.

This policy applies to all Board Members, staff, volunteers, and partners involved in delivering the Award in Nepal. It governs the handling of personal data collected from participants, staff, volunteers, and third-party suppliers.

The Data Protection Leads for the NAO is **Ms. Baybina Shrestha**, Senior Operations and Programme Officer (Baybina.doeia@gmail.com)

Key Principles

The NAO's approach to data protection follows the seven key principles

- **Transparency:** Individuals must be informed about the personal data we collect and how it is used, through clear and accessible privacy notices.
- **Purpose Limitation:** Personal data will only be used for the purposes communicated during collection and for lawful activities.
- **Data Minimization:** We will only collect the necessary amount of personal data required to achieve the stated purposes.
- **Accuracy:** All personal data will be kept accurate and up to date.
- **Storage Limitation:** Personal data will only be retained for as long as necessary and will be securely deleted when no longer needed.

- **Integrity and Confidentiality:** We will implement security measures to protect personal data from unauthorized access or loss.
- **Accountability:** Award Nepal is responsible for complying with these principles and maintaining appropriate measures to demonstrate compliance.

Lawful Bases and Consent

The NAO will process personal data only where there is a lawful basis- a legitimate reason that allows NAO to collect, process and use personal data as established by regulations to ensure that privacy rights are respected and that personal data is handled in a transparent and appropriate manner, including:

- Consent from the individual
- Performance of a contract

Consent from the individual-As part of the registration process on the Online Record Book (ORB), Award participants are asked whether they consent to the use of their photographs they upload to the ORB for promotional materials related to The Duke of Edinburgh's International Award Nepal.

By uploading photographs to the ORB and not opting out during the registration process, participants are deemed to have provided their implicit consent for the use of these images in promotional and marketing materials, both online and offline. However, participants retain the right to withdraw this consent at any time by contacting the Data Protection Lead or their Award Leaders in writing.

The NAO will respect the preferences of participants regarding the use of their photographs and will ensure that any promotional use of photographs is in line with our data protection and privacy obligations.

Performance of a contract- This basis applies when the processing of personal data is necessary for fulfilling a contractual obligation between the individual and NAO.

Examples of processing under this basis include:

- **Registration and Participation:** When a participant register for the Award, we process their personal data to manage their participation. This includes recording their progress in the Award, verifying their achievements, and providing support throughout the Award journey. Without such processing, we would be unable to deliver the Award as agreed in the registration process.
- **Award Completion and Certification:** Upon successful completion of the Award, we process the personal data necessary to issue certificates and ensure proper recognition of achievements. This is essential to fulfilling our contractual obligation to the participant.
- **Event Participation:** When participants attend Award-related events, such as trainings, workshops or Award ceremonies, their personal data may be processed to facilitate their involvement, including logistics, accommodations, or communications about the event.

For individuals under the age of 18, the consent of a parent or legal guardian may be required to enter into the contract and process their personal data.

Adopting Privacy by Design

The NAO commits to privacy to design- 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.

Any privacy settings must be, by default, set to the most privacy protective setting. The NAO must ensure that the minimal amount of personal data is collected and used through our technology and processes.

Third Party Supplier

The providers of services to the NAO must also adopt appropriate and equivalent security measures in relation to any personal data they process on the NAO's behalf.

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 Protection Lead to ensure contracts are up to date with the most recent data protection provisions.

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

Safeguarding and Special Category Data

Special categories of data are information revealing an individual's racial or ethnic origin, political opinions, religious or other beliefs, sexual orientation. Data about actual or alleged criminal offences, whilst not special category data, is similarly afforded greater protection under the law.

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.

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
- (ii) Only collect special categories of data when it is absolutely necessary
- (iii) The Data Protection Lead should be informed of any planned significant use of special categories of data to verify the legitimacy of such use. The Data Protection Lead will work with you to mitigate any potential risks.

Data Protection Impact Assessment and Data Breaches

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

Where the NAO intend to use personal data in a more intrusive way, the NAO must carry out an initial assessment to consider whether the use is justified. Carrying out a DPIA (Data Protection Impact Assessment) helps to identify and minimize the privacy risks associated with the use of personal data.

The NAO's Data Protection 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 Protection Lead on whether a DPIA is required or not.

If you become suspicious or are actually aware of any data security breach, you must immediately report the breach to the Data Protection Lead so that the Data Protection Lead can take protective measures that can effectively mitigate the consequences of the breach

Audits, Compliance and Trainings

Periodic audits will be conducted to ensure compliance with this policy. Reviews for NAOs, will normally be carried-out as part of the Foundation's regular License Review process.

Maintenance and Contact

The review and maintenance of this Policy is the responsibility of the NAO's Data Protection Lead. Queries and feedback should be directed to the NAOs Data Protection Leads:

Baybina Shrestha

(Baybina.doeia@gmail.com)

This Policy may change from time to time – for example, to take into account changes from the Foundation or to reflect changes in regulation or legislation.