Data Protection Impact Assessment Policy

Article 25 is clear that:

"the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

Owner: NA/**W**AA/**K**LF/**6**NA

Date Created	Date 1st Review Due	Date Reviewed	Version	Next Review Due
May 2018	May 2019	May 2019	2	May 2020
		October 2020	3	October 2021
		February 2021	4	February 2022

Purpose
This policy and procedure establishes a process designed to help The Green Room systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of our accountability obligations under the GDPR UK, and demonstrates how we comply with all of our data protection obligations.

Scope
Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing, that is likely to result in a high risk to the rights and freedoms of individuals.

Policy Statement
A DPIA aims to systematically and comprehensively analyse our data processing and help us to identify and minimise data protection risks.
DPIAs consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

When is a DPIA necessary?
Staff must conduct a DPIA before beginning any type of processing which is "likely to result in a high risk".
In particular, the GDPR UK says you must do a DPIA if you plan to:
- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale;
- systematically monitor publicly accessible places on a large scale.

The ICO also requires you to do a DPIA if you plan to:
- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or

- process data that might endanger the individual's physical health or safety in the event of a security breach.

How to carry out a DPIA

A DPIA should begin early in the life of a project, before processing has even started and should include these steps

1 Identify a need for a DPIA
2 Describe the processing
3 Consider consultation
4 Assess necessity and proportionality
5 Identify and assess risks
6 Identify measures to mitigate risks
7 Sign off and record outcomes
8 Integrate outcomes into plan
9 Review

To help with this please refer to the Data Protection Impact Assessment template

Responsibilities

- The overall responsibility for ensuring compliance and performing data protection Impact Assessments activities at The Green Room lies with the Data Protection Officer
- All staff that deal with personal data are responsible for processing in compliance with The Green Room policies and procedures.
- Staff must maintain any necessary records of compliance

This policy is approved by the Co-CEO of The Green Room Foundation

Co-CEO

Date_____