Data Protection Impact Assessment (DPIA) Procedure

Data Controller: Dudley Netball League

Data Protection Lead: Dudley Netball League Honorary Secretary
Email: http://www.dudleynetball.co.uk/

1.0 **Introduction**

1.1 In accordance with the GDPR, we are required to carry out a Data Protection Impact Assessment for all projects that involve processing personal data and any activities (both internal and external) that affect the processing of personal data and impact the privacy of individuals.

2.0 **Purpose**

2.1 The purpose of this procedure is to ensure that you know when and how to conduct a DPIA on projects, systems, technology and processes in order to establish if the processing activities will have an impact on the rights and freedoms of data subjects. This procedure functions in conjunction with the DPIA Tool.

3.0 **Roles & Responsibilities**

3.1 This procedure applies to all Dudley Netball League workforce involved with the processing of personal data who are responsible for performing necessary checks to establish the need for conducting a DPIA.

If you are responsible for introducing a new, or modifying an existing, system, process or technology involving personal data, you must conduct a DPIA to identify any risk to the rights and freedoms of data subjects, BEFORE proceeding with that system, process or technology.

3.2 The Data Protection Lead, assisted by Dudley Netball League Committee, is responsible for approving all DPIA and to ensure that appropriate controls are implemented to mitigate any risks identified as part of the DPIA process.

4.0 **Procedure**

4.1 **Identify the need**

If you are creating or implementing a new project or process; or making significant changes to existing projects or processes, you are required to complete the screening questions in the DPIA Tool. If the answer to any of the questions is YES, you must conduct a DPIA.

4.2 **Describe information flows and how the project satisfies the principles of the GDPR**

You are required to describe the flow of information as it will be carried out under the project, alongside other relevant information including details of the personal data to be collected, the basis for its lawful processing and any other information. The Data Protection Lead or a member of the Data Protection Steering Group can support you to do this.

4.3 Identifying the privacy and related risks

As you go through the full DPIA process, you will get an idea of the risks relating to your project, process or system that will have an impact on individuals. This may be based on the nature of the personal data being processed, the volume of the data, or the manner in which it is being processed, for example. These risks should be logged and assigned a risk rating based on the likelihood of occurrence.

4.4 Identifying and selecting privacy solutions

The level of security controls that you adopt will depend on the risk level. These are classified as high risk, risk and low risk. There are several ways to address a risk including to eliminate, reduce, mitigate or accept the risk. You should consult the Data Protection Lead to ensure that there is a balance between the amount or type of risks that your organisation is prepared to pursue, retain or take.

4.5 Approving the DPIA

As the final stage of a DPIA, you must create a report that summarises the process and the steps taken to address the risks to privacy. Your report must also record decisions taken to eliminate, reduce, mitigate or accept the identified risks. Any privacy risks identified as risk or high-risk, must be approved by the Data Protection Lead.

4.6 Integrating the DPIA outcomes into the project plan

DPIAs will probably generate actions to be taken to address any risks identified or changes to be made to the system, process or technology itself. Therefore, you must evaluate and establish resources to complete these actions. Any actions or solutions identified must be assigned to a specific employee to ensure responsibility and accountability is documented.

5.0 Associated Documents

5.1 This procedure is effective in conjunction with the following associated policies and procedures:

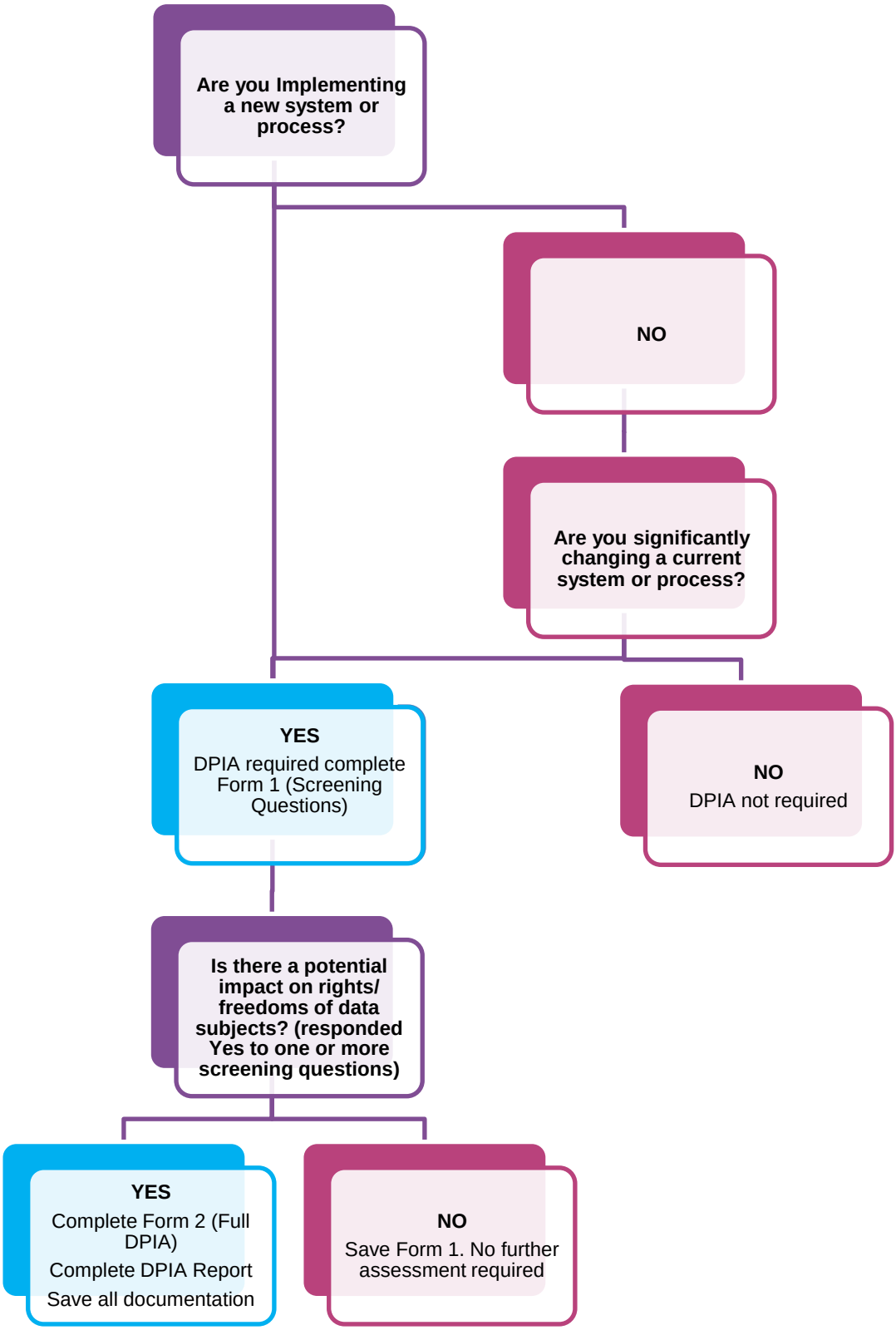
• Data Protection Policy	• Information Security Policy
• Data Sharing Procedure	• Safeguarding Policy • Equity Policy
• Data Subject Rights Procedure	•
• Personal Data Breach Procedure	•

6.0 Definitions

Personal Data	Any information relating to an identified or identifiable person (data subject). An identifiable person is someone who can be identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Special Category Data	Data which requires extra care and precaution to be taken in processing and which details or consists of: • Racial or ethnic origin of the subject; • Their political opinions; • Their religious or philosophical beliefs; • Whether they are a member of a trades union; • Processing of genetic data; • Processing of biometric data; • Data concerning their health; • Their sexual life/orientation.
GDPR	General Data Protection Regulation – a regulation by the European Parliament intended to strengthen and unify data protection for individuals. The GDPR came into force in the UK on 25 May 2018.
DPL	Data Protection Lead – contact details are: Dudley Netball League secretary
Data Protection Steering Group	Our internal group of members from all areas of the organisation that meet regularly to examine, discuss and make recommendations for the protection of personal data. This is the Dudley Netball League Committee.

Data Protection Impact Assessment Tool

Any project, service or contract that requires a data impact assessment will need to follow the procedure below:



FORM 1 (Screening questions): Contains a short screening questionnaire to be completed by someone who knows about the project/service and of the relationship with the third party. If information is unknown, the third party will need to be contacted. If there is no potential impact on the rights and freedoms of data subjects, the DPIA process can end here and be stored centrally to evidence that due diligence has been conducted.

FORM 2 (Full DPIA Questionnaire): Where an impact is likely (by answering 'yes' to any of the screening questions in Form 1), Form 2 will need to be completed.

DPIA Report: The Data Protection Lead or an appropriate senior individual will need to sign the full DPIA once completed. A 'DPIA Report' will also need to be completed. Again, this will be saved, stored centrally and monitored.

Note: Some details will need to be completed by the third party

Form 1: Screening Questions

Data Protection Impact Assessment (DPIA) Screening: <Project/Service/Contract>
Describe project/process, along with the objectives and benefits

Screening Questions	**Yes/No**
Does the project involve collecting new information about individuals?	
Will information about individuals be disclosed to organisations or to people who have not previously had routine access to the information?	
Does the project involve using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in decisions or acting against individuals in ways which could have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, disability and vulnerability records or other information that people would consider to be particularly private.	
Will the project require contact to individuals in ways which they may find intrusive?	

Form 2: Full DDPIA Questionnaire

Data Protection Impact Assessment (DDPIA) Questionnaire: <Project/Service/Contract>

*Other Organisations involved?

Section 1: General Information	Organisation Name	*
	Organisation Address	*
	Name and contact details (email/phone) of the person submitting the response	*
	Organisation Overview	*

Section 2: Data being Processed Please indicate if any or all of this Personally Identifiable Information (PII) is or will be processed	**Yes/No**	**Data Type**	**Yes/No**	**Data Type**
		Name, Address, DOB, Phone, Email		Location data
		Financial information		Disabilities
		Medical/Health information		Biometric or genetic information
		Information about behaviour		Profiling
		Criminal offences/convictions		Other (please specify)
		Religious Beliefs, Trades Union Membership or Political Opinions		Other identifiers e.g. username, twitter name etc.
		Photographs		

Section 2.1: Lawful Bases for Processing Please select which lawful bases for processing apply to the personal data identified as being processed in section 2.	**Yes/No**	**Lawful Bases**	**Additional Information**
		Processing is necessary for the performance of a contract with the data subject or to take steps to enter a contract. e.g. Employment Agreement	
		Processing is necessary for compliance with a legal obligation e.g. Safeguarding Laws	
		Processing is necessary to protect the vital interests of a data subject or another person	
		Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	
		Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (please specify what the legitimate interests are in Additional Information)	
		Consent of the data subject	
		Other (please specify in Additional Information)	

Section 3: Data Flow Please demonstrate how data is accessed, moved and saved.	*Please provide the following information:* ***Where does data go?*** *Please outline how information moves from and to each of the devices and processes* ***Clarify how you encrypt data and when you do so.*** ***Where is the data to be stored/held?*** ***Where are devices that can access the data physically located*** ***How will it be stored?*** ***Will the data be available on the 'cloud'?*** ***How long will it be kept?*** ***How will it be deleted after use?***

Section 4: Data Subject Rights Please clarify how you can offer Data Subjects the following rights *You can reference to your Data Subject Rights process if appropriate*	Right to access	
	Right to have data rectified or erased	
	Right to restrict processing	
	Right to object to processing, automated decision making and profiling	
	Right to object to processing for the purposes of direct marketing	
	Right of data portability	*only applies if data held electronically
	Right to object to processing for scientific, historical or statistical purposes	

Section 5: Breach Notification Please describe your	*You can reference to your Security Incident / Breach process if appropriate*

data breach notification process	

Section 6: Data Transfers (Outside of EU/EEA) If any, please inform of any data being transferred outside of the EU/EEA and the technical and operational measures in place. Please also include any cloud-based data transfers.	

Section 7: Training and Awareness Please confirm how you ensure your workforce meet and understand their data protection obligations.	*You can reference to your Data Protection Policy if appropriate*

Section 8: Sub-Processors Please list any other organisations that you may engage with to further process personal data	

Section 9: Contractual Terms Please provide us with a copy of any data processor agreement or terms relating to data protection	

4. DPIA Report

DPIA Report	
Introduction and overview Summary of Project/Service/Third Part Arrangement.	
The Privacy analysis i.e Information collection and obtaining, Use, Disclosure and retention of information.	
Privacy Risk Assessment outcomes High Risk/Risk/Low Risk.	
Privacy responses Document any responses received from 3rd parties regarding the processes that have been reviewed.	
Compliance mechanisms Document the effectiveness of the processes that have been utilised regarding compliance.	
Conclusion Executive summary of the analysis and compliance – Note: this report must be authorised by Data Protection Lead.	