DATA PROTECTION POLICY

1.0 Introduction

Douglas may collect, process and store sensitive, and personal sensitive data, on an on- going basis. The Data Protection Acts 1988, 2003 & the General Data Protection Regulation EU/2016/679 confer rights on individuals as well as additional responsibilities on those persons and organisations processing any personal data. This policy applies to all data held by Douglas. This includes electronic and paper records; it also includes all CCTV images.

2.0 Ownership

This Data Protection Policy is maintained by the Douglas Executive Secretary-Data Protection Officer (DPO) and is approved by the Club's executive committee. The policy will be reviewed at least annually by the DPO to ensure alignment to appropriate risk management requirements and its continued relevance to current and planned operations, or legal developments and legislative obligations. Further comments or questions on the content of this policy should be directed to the DPO. Any material changes to this policy will require approval by the Executive Committee.

3.0 Scope of Policy

This policy has been drawn up by Douglas and as such is applicable to all Douglas employees (i.e. staff and contractors), mentors, and relevant third parties. All employees and mentors have a personal responsibility to ensure compliance with the principles of all the Data Protection Acts and to adhere to Douglas Data Protection Policy.

Douglas Executive Committee are responsible for ensuring compliance with Douglas Data Protection Policy. They are also responsible for ensuring that all staff and mentors in the club are fully aware of the policy. The Douglas Data Protection Policy applies to data records of all types regardless of the medium on which they are held. The following list highlights the type of data that constitutes as personal data and is covered by the Data Protection legislation (this list in indicative only, and is not intended to be exhaustive):

- Personal data is defined as "Any information relating to an identified or identifiable natural person (data subject)" i.e.
    - Name, date of birth, PPSN, private address.
    - Employer, business address, qualifications, work experience.
    - Contact details.
    - Marital/family status.
    - Employer information/self- employed information.
    - Bank details, income, creditors details, benefits.
    - Details of assets and property, investments, liabilities.
    - IPS address.
    - Personal Image.
- Sensitive personal data including:
    - Details of convictions relating to fraud, tax offences and settlements, dishonesty,
    - medical information etc.

4.0 Douglas Safeguarding Principles, Measures & Promises

4.1 Obtain and Process Information fairly:

Douglas is committed to collecting information fairly and ensuring that it is processed fairly. Douglas is committed to only collecting personal data necessary to allow it to carry out its functions as set out in legislation.

Regarding personal data, Douglas acknowledge that the data subject has the right to the following information:

- Period for which the personal data will be stored
- The existence of their right to request access, rectification, to object to processing and or erasure of their personal data or the restriction of processing their data, as well as the right to data portability
- The existence of their right to place a complaint with the Supervisory Authority
- Whether the provision of personal data is a statutory or contractual requirement
- The existence of any automated decision-making, including profiling

4.2 Keep it only for specified, explicit & lawful purposes:

Douglas will only keep personal data for the purposes that are specific, lawful, and clearly stated at the time of collection and under the consent of the data subject, where applicable

4.3 Use & disclose it only in ways compatible with these purposes:

If data such as "personal data" is obtained by Douglas for a particular purpose then, subject to limited exceptions, the personal data will not be used or disclosed for any other purpose other than that for which it was obtained.

4.4 Keep it Safe & Secure:

Douglas implements appropriate physical, technical, and organisational security measures against unauthorised access to, alteration, disclosure, destruction, or unlawful processing of data and against the accidental loss or destruction of such data. Douglas employees and mentors' access to certain data held by Douglas is restricted on a need-to-know basis and is reviewed periodically. When sharing Clubforce member information internally, we will password protect the file and send the password via a separate medium.

4.5 Ensure that it is adequate, relevant & not excessive:

Personal or Sensitive Data will not be collected or retained if it is not needed and / or on the basis that it might be required in the future. The types of information about individuals that Douglas collects will be reviewed periodically to ensure compliance with this requirement.

4.6 Keep it accurate & up to date:

Douglas will ensure that all Personal data is accurate, complete, and up to date. Any inaccuracies will be remedied as soon as possible.

4.7 Retain it for no longer than is necessary:

Personal and or Sensitive data will not be retained for no longer than is necessary for the purpose(s) for which it is acquired. Data may not be retained indefinitely.

4.8 Right of Access, Rectification, and or Deletion to Personal Data:

Individuals (including Douglas employees and mentors) have the right to access, request rectification, object to processing of their information, restrict the processing of their information and or deletion to any personal data held within Douglas. Douglas will endeavour to ensure that a response to such requests is given, no later than 30 days from the receipt of request.
The right to access, request rectification, object to the processing of their information, restrict the processing of information and or deletion to any personal information does not include a right to see any personal data about any other individual(s), without that other person's consent, to protect their personal rights. Douglas will not disclose any information about any other person during such requests.
Douglas will execute and exercise the rights of all data subjects to the fullest in accordance with legislation

4.9 Transfer to third countries or international organisations

Douglas, nor any Douglas employee or mentor, will not transfer any personal data to any third country or any other international organisation outside of Douglas except in limited circumstances as set out in the Record of Processing

4.10 Record of Processing:

Douglas shall maintain a record of its processing activates under its responsibility. The record shall contain all of the following information.

- Name, contact details of Douglas and the details of the Douglas Data Protection officer
- The purpose of processing
- A description of the categories of data subject and the categories of personal data held
- The categories of recipients to whom personal data has been or will be disclosed, including, recipients in third or international organisations
- Where possible, a general description of the physical, technical, and organisational security measures implemented by Douglas to ensure that safety and compliance with all Data Protection legislation

4.11 Data Breach & Communication:

In the unlikely event of a Personal data breach, and unless Douglas can demonstrate, in accordance with the accountability principle, that the personal breach is unlikely to result in a risk to the rights and freedoms of person affected. Douglas, as soon as have become aware that a personal data breach has occurred, shall notify the Supervisory Authority without any undue delay and will do so in a 72 hour timeframe or less
All Douglas employee's/mentors must upon discovery, and or suspicion of a potential personal data breach notify the Douglas Executive Committee and the appointed DPO in writing within a 30 minute timeframe

4.12 Compliance & Monitoring:

Douglas shall appoint a designated Data Protection Officer (DPO) for the purposes of monitoring compliance with all Data Protection legislation.

The responsibilities of a DPO in accordance with the GDPR (EU/2016/679) are to "assist the controller or the processor to monitor internal compliance with this regulation". As such, the DPO's responsibilities will include, but is not limited to the monitoring the on-going data processing and storage of personal data via;

- Collection of Information to identify processing activities
- Maintaining a record of processing operations
- Analysing and monitoring compliance of processing activities with all Data Protection legislation, GDPR & internal Policies, and procedures
- Conducting Data Audits
- Conducting Privacy Impact Assessments as necessary.

All Douglas employees and mentors will facilitate, comply and adhere to all Douglas internal policies and procedures to ensure the compliance and monitoring framework of the DPO functions efficiently.

5.0 Data Protection Breach

Any loss of personal data in paper or digital format will be responded to and managed in accordance with Douglas Data Security Breach Policy & Procedures and in compliance with the provisions set out all applicable Data Protection Legislation

In order for Douglas to be able to comply, it is essential that all incidents (including suspected incidents) which give rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data are reported without delay to the DPO within a 30 minute timeframe. Incidents can include:

Minor incidents which do not actually result in unauthorised disclosure, loss. Destruction or alteration of personal data
Major incidents for example: Loss or theft of devices such as laptops; unauthorised access to Douglas environment
A Data Protection breach can happen for a number of reasons, e.g.:

- Loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises)
- Loss or theft of documents
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human Error
- Unforeseen circumstance such as a flood or fire
- Cyber-attacks (hacking)
- Obtaining information from the organisation by deception
- Misaddressing of e-mails
- Improper dissemination of information

In the event of a data breach happening, the DPO must be notified immediately and within a 30-minute timeframe. It must not be assumed that someone else has already notified of a breach.

The breach should be notified using the official Personal Data Security breach form set out in Appendix 1 of the Personal Data Security Breach Procedures.

The DPO will assess the breach and make a decision on the next steps to be taken in accordance to the Douglas Data Breach Response Policy.

Following review of a breach by the DPO, if the data breached affects the rights and freedoms of a data subject, the DPO will inform the Office of the Data Protection Commissioner within a 72-hour timeframe of Douglas becoming aware of the breach.

6.0 Training

Data Protection Training will be provided through staff / mentor presentation during inductions when employees commence employment with Douglas One Club. Refresher Data Protection training will be delivered on an at least annual basis to all employees and will be augmented by online material and information notices where appropriate.

7.0 Douglas Employee Agreement

All Douglas employees agree to adhere fully to the Douglas Data Protection Policy and all additional policies and procedures. Failure to comply with any of the safeguards, policies, procedures or directions from management or the DPO may follow an investigation and may lead to disciplinary action in accordance with Douglas disciplinary procedures

5. Specific data retained, controls and retention period

Data	Data Owner	Processor	Controls in place	Retention Period
Registrations	Douglas	Clubforce	GDPR compliant	Until membership ends
Payroll	Douglas	Accounting Firm	GDPR compliant	Per legislation
Player contact Data	Douglas	Mentors	Password protected files	Until membership ends

6. Reference Information

- Guidance on the Use of CCTV – For Data Controllers (Data Protection Commission)