**Procedure checklist**

**This template is designed to cover the policy issues relating to GDPR that are pertinent to organisations delivering sport/physical activity.**

**It has been designed to be adapted and amended to reflect the scope, activities, and procedures of your organisation. It also outlines the procedures that should be carried out to ensure compliance with the policy.**

**Items in green should be amended to reflect your group and your processes.**

**Once amended and finalised by agreement of your management to reflect your organisation it should be read by officers, staff, volunteers to inform them about GDPR procedures.**

**Disclaimer: Please remember that our resources reflect core governance principles and good practice but do not constitute legal advice.**

**DP officer = data protection officer**

**DP officer = data protection officer**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ref** | **Objective** | **Control 1** | **Control2** | **Control 3** | **Control** |
| 1 | **Legal accurate records** |  |  |  |  |
| 1.1 | Collect the minimum of personal information | Document the personal information that must be collected for each type of data subject and reasons why data is collected:  Staff, Officer, Volunteer  Member, member under 18 | Nominated officer  develops template (a) for each type of data subject | Nominated officer confirms templates have been developed | Progress reported to senior managers / trustees / directors / management committee |
| 1.2 | Don’t collect extra information just because it might be helpful later | Review template (a) for each type of data subject annually or after data incident to ensure only appropriate information is collects | Nominated officer  carries out the review of the template | Nominated officer reports templates have been  reviewed | Progress reported to senior managers / trustees / directors / management committee |
| 1.3 | Will not keep data longer than we need to. | Annual review that personal data held is accurate, appropriate, complete, and up to date | Nominated officer  carries out the review | Nominated officer  officer reports on  review | Progress reported to senior managers / trustees / directors / management committee by DP Lead |
| 1.4 | Appropriate data is collected when individuals join the club | Template used to collect data at member registration, or when staff volunteer or officer joins the club | Nominated officer  updates data from member registration docs etc. to club records | Appropriate officer checks records against membership list (monthly) to ensure they have been updated |  |
| 1.5 | The accuracy and propriety of data held is checked annually | Nominated officer appointed to  review all personal data held to ensure it is accurate, appropriate, complete, and up to date | Data subjects informed of what data is held and asked to identify errors etc | Nominated officer  reports when  review is completed | Progress reported to senior managers / trustees / directors / management committee by DP Lead |
| 1.6 | Amendments are made within 7 days to correct any errors etc | Nominated officer is appointed to update all personal data from Data subjects’ amendments | Data subjects’ information is updated and amended where errors etc. identified | Nominated officer reports  amendment completed | Progress reported to senior managers / trustees / directors / management committee by DP Lead |
| **2** | **Informed staff and members** |  |  |  |  |
| 2.1 | Review of data protection policy, Privacy notice and procedure checklist annually | Officer with appropriate knowledge and skill is assigned to review the policy and procedures | Timescale and resources given to assigned officer | Officer reports review completed, and amendments made. Version control update | DP Lead reviews amendments and reports to senior managers / trustees / directors / management committee |
| 2.2 | Personal data is be deleted within 12 months of members leaving the club. | Nominated officer is assigned to maintaining Leavers list | Leavers list is used by officer validating data at 1.5 | Nominated officer confirms review completed and reports amendments | Progress reported to senior managers / trustees / directors / management committee by DP Lead |
| 2.3 | Personnel records are maintained in line with the requirements of statutory agencies e.g. HMRC  (if staff are employed on PAYE etc) | Manager responsible for personnel issues confirm the retention requirements for staff records with HMRC etc. | Record retention schedule developed for each type of data subject. Data checked at 1.5 | Manager responsible confirms that retention of records is in line with the retention schedule | Progress reported to DP Lead |
| 2.4 | We keep clear records of what action we have taken, and what steps taken to protect the data. | Nominated officers to take relevant action as per Control 1 column |  | Records maintained and reports made by Nominated officer as per column 3 |  |
| 2.5 | Someone is assigned to take responsibility for GDPR as data protection lead | Someone is nominated as the DP lead | Policy and Privacy notice updated with DP lead details |  |  |
| 2.6 | DP lead has the resources and training to understand the organisational, legal, and technical issues involved | Training and information needs assessment carried out for DP Lead | Training and information resources secured for DP Lead | DP Lead accesses training | Progress reported to senior managers / trustees / directors / management committee by DP Lead |
| 2.7 | DP Lead reports annually on compliance with GDPR directly to senior management | DP Lead identifies reporting requirements for senior management | GDPR annual report is drafted for SMT meeting prior to the AGM |  | Information on GDPR presented to the AGM |
| 2.8 | Report on compliance with GDPR directly to senior management regularly or after any significant data incident | DP Lead identifies reporting requirements for senior management | GDPR is set as a standing item on senior management meeting agenda | DP Lead collates reports on GDPR issues arising | Information on GDPR is minuted in senior management meeting minutes |
| 2.9 | Assign a deputy to support the data protection lead, who has appropriate knowledge and training | Someone is nominated as the DP deputy lead | Training and information resources secured for DP deputy Lead | DP deputy Lead accesses training | Progress reported to senior managers / committee by DP Lead |
| 2.10 | Secured training and information for all officers, staff, and volunteers to make sure they are aware of the importance of data protection and understand the procedures they must follow | Training and information needs assessment carried out for officers, staff, and volunteers. Policy and privacy notice provided to all | officers, staff, and volunteers confirm that they have read and understand policy and their responsibilities | Officers, staff, and volunteers confirm that they give consent for their personal data to be used by the organisation | officers, staff, and volunteers understanding and consent included in reporting requirements at 2.8 |
| **3** | **Data security** |  |  |  |  |
| 3.1 | Established appropriate security measures, to protect against unlawful or unauthorised processing, and against loss, destruction, or damage | Nominated officer to carry out risk assessment for secure storage collection and processing of personal data. Identify appropriate effective and sufficient controls | Assess effectiveness of risk control measures annually by testing controls in place and working | Assess effectiveness of risk control measures after significant data incident | Progress reported to senior managers / committee |
| 3.2 | Technical security controls are in place to protect against theft or loss of data, on computer systems | Record of IT security measures maintained by nominated officer, including technical manuals | Measures to include encryption, passwords, firewalls, and anti-virus software | Assess effectiveness of controls by testing controls are in place and working | Progress reported to senior managers / committee |
| 3.3 | Physical security controls are in place to protect against theft or loss of data, either on computer or paper-based systems. | Record of IT security measures maintained by nominated officer | Measures to include locked premises, alarms, cameras locked cabinets | Assess effectiveness of controls by testing controls are in place and working | Progress reported to senior managers / committee |
| 3.4 | Security controls are in place to protect against theft or loss of data where data is stored on mobile technology | Record of IT security measures maintained by nominated officer of laptops and smartphones etc. that are used to store club data outside club premises (e.g. for homeworking | Measures to include passwords, firewalls, and anti-virus software Locking away or out of view in vehicles | Assess effectiveness of controls by testing controls are in place and working | Progress reported to senior managers / committee |
| **4** | ***Security incident*** |  |  |  |  |
| 4.1 | XX will report any data breach that is likely to harm individuals to the Information Commissioners Office, because personal data has been put at risk, e.g. loss of data corruption of data, inappropriate disclosure of data  . | Nominated person and procedures in place to report to the Information Commissioners Office   * in 72 hours of becoming aware of it, * providing information on what has happened, including what data and individuals are at risk, and * what we are doing about it | Nominated person to investigate incident to identify what has happened, including what data and individuals are at risk, and to determine what remedial action is needed to recover the data and prevent further breach | Nominated person to inform the police if incident involves the theft of IT equipment or break into premises | Progress reported to senior managers / committee |
| 4.2 | We will inform individuals impacted by data breach  if they have been put at high risk for example, if a hacker may have gained access to credit card details or be able to commit identity fraud.  without undue delay and give clear information on what has happened. | Nominated person to investigate incident to identify what has happened, including what data and individuals are at risk, and to determine what remedial action is needed to recover the data and prevent further breach |  | Nominated person to inform individuals impacted by data breach confirming impact of breach and action to be taken by the individual | Progress reported to senior managers / committee |