**Data Protection and Data Management Outline Table**

***This outline document needs to be amended as required to suit your specific needs, it can be used to allow drafting of a data protection policy and the associated management process to be used***

* *Change the logo in the Header to your own*
* *Use the select all then replace all to amend the document for your NGB*
* *If your NGB is an unincorporated organisation i.e. not a Company replace all reference to the Board of Directors with the name of your NGB governing committee e.g. Executive or Management Group*
* *If your NGB is a charity your governing group may be the Trustees or similar*

*The table below briefly outlines why data protection and data management is important. It is not a requirement for a not for profit organisation to be registered with the Information Commissioner’s Office but it is good practice and shows your members and stakeholders that your organisation is serious about the management of the data it holds.*

| **Data Protection and Management** | | |
| --- | --- | --- |
| **Policy information** | | |
| **Organisation:** | **Insert NGB Name** | **Additional notes** |
| **Scope of policy:** | Decide on the scope of the policy  e.g. The policy as adopted applies to all officers, committee members, coaches, team managers and volunteers | Amend the list of people as required to suit specific needs of NGB, include employees if appropriate – remember to link to employee handbook and any other handbooks or policies that are impacted by data management |
| **Policy operational date:** | Write the first draft and circulate for comment and then final Board approval. | Board members to return comments - *insert name and date* |
| **Date approved by the Board:** | Once agreed set review date in the Board calendar and agree process to monitor the management of data including delegation of duty as appropriate | CEO or other identified person checks the access to sensitive personal data such as names and addresses of athletes etc. and ensures that it is only accessed by approved individuals |
| **Policy review date:** | Every 2nd year following its approval date or sooner if required | Responsibility of ……*insert person* *who will undertake the review and set it for Board approval* |
| **Background Information** |  | **Additional notes** |
| **Purpose of policy:** | The purpose of this policy is to enable the NGB to:   * comply with the law in respect of the data it holds about individuals; * follow good practice; * protect the NGB’s officers, athletes and other individuals associated with our sport; * protect the NGB from the consequences of a breach of its responsibilities | Add in any other reasons that the Board might identify as the reason for a data management policy and process e.g. to follow agreed policy of international federation or similar; to comply with anti-doping regulations etc. |
| **Data Protection Principles:** | There are 8 main principles covered by the Data Protection Act:   1. Fairly and lawfully processed 2. Processed for limited purposes 3. Adequate, relevant and not excessive 4. Accurate and up to date 5. Not kept for longer than is necessary 6. Processed in line with your rights 7. Secure 8. Not transferred to other countries without adequate protection | |
| **Personal data:** | The NGB policy should apply to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of ‘data’ in the Act. A decision needs to be made about what the NGB considers as its ‘data’. | Suggest consideration is given about how different data is stored and where it is stored e.g. membership names, addresses, bank details; athletes data for anti-doping etc.; volunteers data.  Do not leave matters to chance – manage how your NGB data is stored, used and accessed. |
| **Rights of Individuals:** | The Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records. Should an individual or organisation feel they are being denied access to personal information they are entitled to, or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office for help. | Consider how the NGB will deal with requests from individuals about the data held by the NGB about them. Who should requests be sent to, what timescales will be followed? |
| **Policy statement:** | The NGB needs to include reference to the previous points and commit to:   * comply with both the law and good practice * respect individuals’ rights * be open and honest with individuals whose data is held * adopt a policy on the secure storage, handling, use, retention and disposal of information including Disclosure Information in accordance with DBS | The actual policy wording should contain reference to the four bullet points as a minimum, others points may be added to suit your individual NGB needs. |
| **Code of Practice for NGB data handling:** | The NGB must recognise that its first priority under the Data Protection Act is to avoid **causing harm to individuals.** In the main this means keeping accurate information securely in the right hands. | Link data handling about bank accounts etc. to the NGB anti-fraud policy and procedures  Consider signing up for the “Personal Information Promise” – further details can be found at:  https://ico.org.uk/for-organisations/improve-your-practices/personal-information-promise/ |
| **Key risks:** | The NGB must consider the main risks of not having or not complying with a data management process  e.g.  The main risks within the NGB fall in two key areas:   * information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information * individuals being harmed through data being inaccurate or insufficient | Examples of identified risks might include the following:   * Breach of confidentiality * Insufficient clarity about the range of uses of the data — leading to volunteers, athletes etc. being insufficiently informed * Failure to offer choice about data use when appropriate * Breach of security by allowing unauthorised access * Failure to establish efficient systems of managing changes to data - leading to data not being up to date * Harm to individuals if personal data is incorrect * Insufficient clarity about the way personal data is being used e.g. given out to general public/media * Information given out on a website without consent |
| **Responsibilities of Each Person within the Procedures** | | |
| **Category/Person** | | **Additional notes** |
| **Board:** | The Board has overall responsibility for ensuring the NGB complies with its legal obligations. The NGB needs to agree who (there can be more than one) will be the named Data Controller (s) – this is important if registering with the ICO | Include details in the Board annual delegation authority  Information Commissioners Office website: https://ico.org.uk/for-organisations/ |
| **Data Controller:** | The responsibilities of the Data Controller include:   * Briefing the Board on Data Protection matters * Reviewing Data Protection and related policies * Advising other staff/volunteers on tricky Data Protection issues * Ensuring that Data Protection induction and training takes place if deemed necessary * Handling subject access requests * Approving unusual or controversial disclosures of personal data * Approving use of data by other Data Processors | If requested, the Data Controller must comply with a police authority to provide required details  The Data Controller may be the CEO or similar with the data processors being admin staff or similar. Some individuals may have access to small amounts of specific data e.g. a team manager most likely will hold information about athletes  If the membership data is stored by another organisation e.g. UK Governing Body then ensure you are fully aware of their data management policy and procedures and how the data provided to your NGB fits within them |
| **Website Manager:** | Where personal data is handled via the website or similar such as online affiliation, the Website Manager should be responsible for electronic security and for approving any Data Protection related statements on web materials | e.g. limit access via a secure part of the site – password protection, issue of logins etc. |
| **Managers of Athletes:** | All volunteer and/or paid Managers should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their duties for the NGB.  This may include athletes’ names, addresses and other contact details as well as medical information. | Managing the people who hold, collate or access the data outside of the “office” e.g. All athlete managers (e.g. coaches, physio/doctors, Chairs of Committees etc.). They should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their duties. It might be good practice to obtain signatures to that effect. |
| **Child Protection Officer:** | Make sure that when writing the policy and procedures reference is given to NGB safeguarding information using suitable wording taken from the applicable regulations. | Note about club welfare officers – link to GB/International websites if appropriate  *To ensure that the safeguarding information in the data management process is kept up to date consider using a link to safeguarding on the NGB website rather than actual updating of the data management process document.* |
| **Members** | It is good practice to encourage the NGB members to also be aware of the way they manage data, this can be very important if for example a club collates the data then passes it on to you. The original data must be accurate and the manner in which it is transferred should be secure. | The NGB may not want to be held responsible for the inaccurate data it receives from e.g. clubs. The design and management of club affiliation forms might need to be carefully worded. |
| **Individuals** | Responsibility for accurate individual data provision needs to be set as the responsibility of the individual who is giving the NGB their own personal data. Same applies to the changing of the data. | A mechanism for individuals to check their data before uploading to a website should be considered to reduce inaccuracy. Individuals should also be encouraged to advise of changes to e.g. email or address as soon as possible after the change as this ensures the NGB information held is up to date. Consider a clause about the NGB not being responsible for out of date information if an individual fails to update their details. |