**THE HANDBALL FOUNDATION – DATA PROTECTION POLICY**

Definitions

GDPR: General Data Protection Regulation
Responsible Person: (Chief Executive Officer)

1. Data protection principles

The Handball Foundation is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

2. General provisions

1. This policy applies to all personal data processed by the The Handball Foundation.
2. The Responsible Person shall take responsibility for the The Handball Foundation’s ongoing compliance with this policy.
3. This policy shall be reviewed at least annually.
4. The Handball Foundation shall register with the Information Commissioner’s Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

1. To ensure its processing of data is lawful, fair and transparent, The Handball Foundation shall maintain a Register of Systems.
2. The Register of Systems shall be reviewed at least annually.
3. Individuals have the right to access their personal data and any such requests made to the The Handball Foundation shall be dealt with in a timely manner.

4. Lawful purposes

1. All data processed by the The Handball Foundation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests
* *You must have a valid lawful basis in order to process personal data.*
* *There are six available lawful bases for processing. No single basis is ’better’ or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.*
* *Most lawful bases require that processing is ‘necessary’. If you can reasonably achieve the same purpose without the processing, you won’t have a lawful basis.*
* *You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.*
* *Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.*
* *If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).*
* *If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.*
* *If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.*

*The Information Commissioner’s Office*
[*https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing*](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing)

1. The The Handball Foundation shall note the appropriate lawful basis in the Register of Systems.
2. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
3. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the The Handball Foundation’s systems.

5. Data minimisation

1. The Handball Foundation shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

1. The Handball Foundation shall take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

1. To ensure that personal data is kept for no longer than necessary, The Handball Foundation shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
2. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

1. The Handball Foundation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
3. When personal data is deleted this should be done safely such that the data is irrecoverable.
4. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, The Handball Foundation shall promptly assess the risk to people’s rights and freedoms and if appropriate report this breach to the ICO

*A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.*

*Example*

*Personal data breaches can include:*

* *access by an unauthorised third party;*
* *deliberate or accidental action (or inaction) by a controller or processor;*
* *sending personal data to an incorrect recipient;*
* *computing devices containing personal data being lost or stolen;*
* *alteration of personal data without permission; and*
* *loss of availability of personal data.*

*A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.*

*Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.*

* + - *The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.*
		- *If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, you must also inform those individuals without undue delay.*
		- *You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.*
		- *You must also keep a record of any personal data breaches, regardless of whether you are required to notify.*

*The Information Commissioner’s Office*
[*https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches*](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches)

END OF POLICY

We request that our Staff, Volunteers, Member and Visitors respect this Policy, a copy of which will be available on demand.

Approved by the Board of Trustees

Updated: April 2024