Women in Sport Data Protection Policy

1. Context & Purpose

Women in Sport exist because we believe women and girls belong in sport and our vision is that no-one is excluded from the joy, fulfilment and lifelong benefits of sport.

As an organisation we are committed to protecting the integrity and security of all data relating to **al**l our stakeholders including but not limited too employees, supporters and funders.

The following policy gives guidance on ensuring all personal information is collected and used appropriately and is kept safely and securely and that we are compliant with all relevant legislation and regulations.

The following policy is based on the General Data Protection Regulation 2018 (GDPR) and its purpose to protect the “**rights and freedoms”** of living individuals and to ensure that personal data is processed with their **informed consent**.

1. Policy

Women in Sport is committed to compliance with all relevant laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information we collect and process in accordance with the GDPR.

The GDPR and this policy apply to all of Women in Sport personal data processing functions, including those performed on employees’, suppliers’, donors’, research participants’ and partners’ personal data, and any other personal data the organisation processes from any source.

The nominated lead for data protection is the Head of People, Finance and Operations at Women in Sport.

This policy applies to employees, staff, consultants and volunteers including any outsourced suppliers. Any breach of the GDPR will be dealt with under the organisation’s disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with WiS who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

No third party may access personal data held by WiS without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which WiS is committed, and which gives WiS the right to audit compliance with the agreement.

1. Definitions
	1. **Personal data** - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 natural person.
	2. **Special categories of personal data** - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
	3. **Data controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
	4. **Data subject** – any living individual who is the subject of personal data held by an organisation.
	5. **Processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
	6. **Profiling** – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.
	7. **Personal data breach** – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.
	8. **Data subject consent** - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.
	9. **Child** – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.
	10. **Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
	11. **Filing system** – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
2. Responsibilities and roles under the General Data Protection Regulation

Women in Sport is a data controller under the GDPR. The GDPR lead and all staff are responsible for developing and encouraging good information handling practices within the organisation. Compliance with data protection legislation is the responsibility of all employees / staff who process personal data.

The GDPR lead has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for employees / staff seeking clarification on any aspect of data protection compliance.

All employees will receive regular GDPR compliance training.

All employees are responsible for ensuring that any personal data about them and supplied by them to WiS is accurate and up to date.

1. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR.

1. Personal data must be processed lawfully, fairly and transparently
2. Personal data can only be collected for specific, explicit and legitimate purposes
3. Personal data must be adequate, relevant and limited to what is necessary for processing
4. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay
5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
6. Personal data must be processed in a manner that ensures the appropriate security
7. The controller must be able to demonstrate compliance with the GDPR’s other principles (accountability)
8. Data subjects’ rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

1. To make subject access requests regarding the nature of information held and to whom it has been disclosed.
2. To prevent processing likely to cause damage or distress.
3. To prevent processing for purposes of direct marketing.
4. To be informed about the mechanics of automated decision-taking process that will significantly affect them.
5. To not have significant decisions that will affect them taken solely by automated process.
6. To sue for compensation if they suffer damage by any contravention of the GDPR.
7. To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
8. To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
9. To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
10. To object to any automated profiling that is occurring without consent.

WiS ensures that data subjects may exercise these right through a data access requests process. WiS will ensure that its response to the data access request complies with the requirements of the GDPR.

Data subjects have the right to complain in related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

1. Consent
2. WiS understands ‘consent’ to mean that it has been explicitly and freely given a specific, informed and unambiguous indication of the data subject’s wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.
3. WiS understands ‘consent’ to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
4. There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.
5. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.
6. In most instances, consent to process personal and sensitive data is obtained routinely by WiS using standard consent documents. e.g. when a new client signs a contract, or during induction for participants on programmes.
7. Where WiS provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16
8. Security of data

All employees / staff are responsible for ensuring that any personal data that WiS holds and for which they are responsible is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by WiS to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security and must be kept:

* in a lockable room with controlled access; and/or
* in a locked drawer or filing cabinet; and/or
* if computerised, access protected in line with corporate requirements and/or
* stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media
1. Disclosure of data

WiS must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All employees, contractors, secondees or volunteers should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of WiS business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the GDPR lead.

1. Retention and disposal of data

WiS shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

WiS may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out when collecting the data which would include statutory obligations.

Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

1. Data transfers

The GDPR restricts transfers of personal data outside the European Economic Area (EEA) unless the rights of the individuals in respect of their personal data is protected in another way or one of a limited number of exceptions applies. All exports of data are unlawful unless there is an appropriate “level of protection for the fundamental rights of the data subjects”.

All staff are required to speak to the Data Protection Lead before proceeding with a data transfer.

1. Risks to data

WiS is aware of any risks associated with the processing of particular types of personal data. WiS shall assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) shall be carried out in relation to the processing of such personal data, and in relation to processing undertaken by other organisations on behalf of WiS.

WiS shall manage any risks identified by the impact assessment in order to reduce the likelihood of a non-conformance with this policy. Appropriate controls shall be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level under the requirements of the GDPR.

Appendix A: General Privacy Policy

1. **Purpose and Background**

**Women in Sport is committed to protecting your privacy and security by ensuring all personal information collected is used appropriately and is kept safely and securely in accordance with our Data Protection Policy.**

**This general privacy policy explains how and why we collect, store and use your personal information.**

* We will only use your personal data with your consent, for purposes for which it was obtained.
* We also continually review what information we hold and will delete personal data which is no longer required.
* We will only share your personal information in order undertake services or when we are required to do so by law.
* We do not sell, trade or rent your personal information to others.

This policy should be read together with our Data Protection and Complaints Policies which are available on our website.

1. **Definitions**
	1. **Personal data:** information that identifies a living person, or which can be identified as relating to a living person. When we talk about “you” or “your” in this policy we mean any living person whose personal data we collect.
	2. **Data Controller is a person or legal entity who controls how personal information is processed and used.**
	3. **Data Processor is a person or legal entity who process and uses personal information in accordance with the instructions of a third party i.e. the Data Controller.**

**We may, depending on the circumstances, act as a Data Controller and or a Data Processor. When we act as a data controller, you will be able to exercise your rights in relation to your personal information with us. When Women In Sport is the Data Processor, that means you cannot exercise these rights against us directly.**

**In such circumstances, we will endeavour to inform you who is the Data Controller of your personal information so that you can direct any such requests to them.**

1. **Your personal data**
	1. We obtain personal data when you:
* inquire about our activities
* sign up to any of our services including our newsletters, training events.
* donate to us
* when you visit our website[[1]](#footnote-1),
* apply for a job or volunteering opportunity with us
* enter into a contract with us
* contact us for any other information
* through third parties such as from external media sources and through publicly available sources including information from social media
* partners on events, research and other projects
	1. The personal data you provide us as listed in the point above may include:
* Personal information: your name, date of birth, email/IP address, postal address and telephone number, biometric data, & images
* Family spouse/partner/next of kin details.
* Financial information (such as credit/debit card or direct debit details, whether your donations are gift aided).
* Information provided by you in response to an event
* Information provided by you in the form of an enquiry to us.
* Details of the ways in which you wish to be contacted by us.
	1. Examples of personal data generated as a result of your involvement with us
* Enquiries regarding our research, publications and events.
* Your visits to our website.
* Your attendance at our events.
* Your donation history.
* How you have helped us by volunteering or donating to us.
* When you have applied for a job.

Special categories of personal data: we do not normally collect or store special categories of personal data. However, there may be situations when we need to do so. Please contact our Data Protection lead info@womeninsport.org if you wish to clarify the circumstances for collecting special categories of data.

1. **How we use your personal data**
* to provide you with services and products,
* to keep you up to date and informed of our activities including research, campaigns, pilots, solutions, policies and fundraising
* manage our relationship with you
* to send you any other information that you may find useful from WiS
1. **How long do we hold your personal data**

We will only hold your information as per the consent provided, or for as long as required by law. Where you ask us to delete your records, we would delete it earlier.

The duration for which we retain your personal information will differ depending on the type of information and the reason why it was collected. In all instances of collecting your data, we will specify the length of time that we will hold the information.

1. **Security**

We are committed to ensuring that your information is secure. To prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

**Any donations made from our website are processed by a third party (Blackbaud Merchant Services) via a secure online portal. For further details about how Blackbaud Merchant Services keep your information safe and secure, please see their** [Privacy Policy](https://www.blackbaud.com/privacy-policy.aspx)**.**

1. **Control of your personal data**

**You have complete control of your personal data and my use of the following rights established under the GDPR to do so:**

* The right to know whether we hold your personal data and, if we do so, where it is technically feasible to be sent a copy of the personal data that we hold about you.
* The right to have your personal data erased (though this will not apply where it is necessary for us to continue to use the data for lawful reasons).
* The right to have inaccurate data rectified.
* The right to object to your personal data being used for marketing or profiling; and automated decision making
* To withdraw the right to use your personal information in a particular manner

**There are some exceptions to the rights above, or if you would like further information on your rights or you wish to exercise them or wish to make a subject access request please contact our Data Protection Lead at** info@womeninsport.org

1. **Consent**

By providing us with your personal data, you consent to the collection and use of any information you provide in accordance with the above purposes and this privacy statement.

If you believe that any information we are holding on you is incorrect or incomplete, please write to us or email us as soon as possible, at the addresses below. We will promptly correct any information found to be incorrect.

Data Protection Lead
Women in Sport
House of Sport

190 Great Dover Street

London

SE1 4YB
info@womeninsport.org

1. **Changes**

We reserve the right to amend this privacy policy from time to time to ensure that it remains up to date and continues to reflect how and why we use your personal information from our website. Any changes will be posted on this page: <http://www.womeninsport.org/privacy-policy>

1. **Complaints**

**Should you have a complaint about how we have used (“processed”) your personal data, in line with our complaints policy you can complain to us directly by contacting our Data Protection Lead at** info@womeninsport.org**.**

**If you are not happy with our response, or you believe your data protection or privacy rights have been infringed you can complain to the Information Commissioners Office. Details of this can be found at** [www.ICO.org.uk](http://www.ICO.org.uk)

1. **Related policies**
* **Data Protection Policy**
* **Complaints Policy**
* **Whistleblowing Policy**
1. **We use cookies on our website**. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences. You can choose to accept or decline cookies.

**Links to other websites:** Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. such sites are not governed by this privacy statement. [↑](#footnote-ref-1)