The Weir Link's Data Protection Policy

This policy has been agreed and adopted by the Trustees.

Signed by the Chair of the Trustees, Michael G. Hughes **27.10.20**

Policy Review period: 2 years

Reviewed – Autumn 2020

Next review – Autumn 2022

Key legislation

Data Protection Act 2018: General Data Protection Regulation (GDPR)

Contents

1. Aims

The Weir Link aims to ensure that all personal data collected about staff and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR).

This policy applies to all personal data, whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR, it is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Us, We, Our the Company, the Charity shall mean or refer to The Weir Link (company number 5819428, registered charity number 1114855).

Personal data

Any information relating to an identified, or identifiable, individual. This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username
- It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data

Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject

The identified or identifiable individual whose personal data is held or processed.

Data Controller

The Weir Link is the Data Controller. This is the entity that determines the purposes and the means of processing of personal data.

Data processor

A person or other body, other than an employee of the Data Controller, who processes personal data on behalf of the data controller.

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Trustees

The Trustees at the relevant time of The Weir Link.

4. The Data Controller

The Weir Link is the Data Controller and is registered with the ICO as a Data Controller.

The Weir Link will renew registration annually or as otherwise legally required.

5. Roles and responsibilities

a. The Weir Link will ensure it complies with all relevant data protection obligations.

b. Given that The Weir Link processes data on a small scale (both in terms of the amount of data and geographical reach) We have not appointed a Data Protection Officer. The Weir Link's nominated GDPR point of contact (the "**GDPR Contact**") is Lizzie Taczalski, Business Development and Marketing Manager. She is contactable via email lizzie.taczalski@theweirlink.org.uk

c. All staff are responsible for:-

- collecting, storing and processing any personal data in accordance with this policy
- informing Us of any changes to their personal data, such as a change of address
- informing the GDPR contact in the following circumstances:
    - ask questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - where they have any concerns that this policy is not being followed
    - where they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - where they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - if there has been a data breach
    - whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - if they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The GDPR is based on data protection principles that We must comply with. The principles say that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary for the purposes for which it is processed
- processed in a way that ensures it is appropriately secure. This policy sets out how We aim to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

The Weir Link will ensure any personal data is:-

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary;
- 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.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when We first collect their data.

If We want to use personal data for reasons other than those given when We first obtained it, We will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- We need to liaise with other agencies or organisations – We will seek consent as necessary before doing this
- Our suppliers or contractors or staff or volunteers need data to enable Us to provide services to Our staff and children – for example, IT companies. When doing this, We will:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data We share
    - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with Us.

- We will also share personal data with law enforcement and government bodies where We are legally required to do so, including for:
    - the prevention or detection of crime and/or fraud
    - the apprehension or prosecution of offenders
    - the assessment or collection of tax owed to HMRC
    - in connection with legal proceedings
    - where the disclosure is required to satisfy Our safeguarding obligations
    - research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provide

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that The Weir Link holds about them. This includes:

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of the data processing
- the categories of personal data concerned
- who the data has been, or will be, shared with
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter or email to the GDPR Contact. They should include:

- name of individual
- correspondence address
- contact number and email address
- details of the information requested.

9.2 Responding to subject access requests

When responding to requests, We:

- may ask the individual to provide 2 forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 1 month of receipt of the request
- will provide the information free of charge
- may tell the individual We will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- might cause serious harm to the physical or mental health of an individual

If the request is unfounded or excessive, We may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When We refuse a request, We will tell the individual why, and tell them they have the right to complain to the ICO.

9.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when We are collecting their data about how We use and process it (see section 7), individuals also have the right to:

- withdraw their consent to processing at any time
- ask Us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- prevent use of their personal data for direct marketing
- challenge processing which has been justified on the basis of public interest
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- prevent processing that is likely to cause damage or distress
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the GDPR Contact.

10. CCTV

We may use CCTV and/or video recording and/or monitoring equipment ("**CCTV**") in various locations around The Weir Link's site. We adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but We make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the GDPR Contact.

11. Photographs and videos

As part of Our activities, We may take photographs and videos of individuals. We will obtain written consent from parents/carers for photographs and videos to be taken of a child or themselves for internal assessment, display, communication, website and Our social media feed. We will clearly explain how the photograph and/or video will be used to the parent/carer.

Consent can be refused or withdrawn at any time. If consent is withdrawn, We will delete the photograph or video and not distribute it further. When using photographs and videos in this way We will not accompany them with any other personal information about the child, to ensure they cannot be identified.

12. Data protection by design and default

We will put measures in place to show that We have integrated data protection into all of Our data processing activities, including:

- considering whether to appoint a DPO;
- in any event appointing a GDPR Contact
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- integrating data protection into internal documents including this policy, any related policies and privacy notices
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; We will also keep a record of attendance
- regularly conducting reviews and audits to test Our privacy measures and make sure We are compliant

maintaining records of Our processing activities, including:

- for the benefit of data subjects, making available the name and contact details of Our GDPR Contact and all information We are required to share about how We use and process their personal data (via Our privacy notices)
- for all personal data that We hold, maintaining an internal record of the type of data, data subject, how and why We are using the data, any third-party recipients, how and why We are storing the data, retention periods and how We are keeping the data secure.

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- paper-based records are kept under lock and key when not in use
- portable electronic devices, such as laptops, hard drives and iPads that contain personal data are password protected
- papers containing confidential personal data must not be left on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access.
- passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- computers are timed to 'sleep' after 5 minutes of inactivity and require passwords to re-open
- staff who access and store personal information on their personal devices are expected to follow the same security procedures as for The Weir Link equipment
- where We need to share personal data with a third party, We carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, We will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on The Weir Link's behalf. If We do so, We will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The Weir Link will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, We will follow the procedure guided by the ICO.

In the event that full details of the nature and consequences of the data breach are not immediately accessible (*eg:* because Data Processors do not work on every normal weekday) the Trustees will bring that to the attention of the Information Commissioner's Office and undertake to forward the relevant information as soon as it becomes available.

16. Training

All staff are provided with data protection information as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or internal processes make it necessary.

17. Monitoring arrangements

The GDPR Contact is responsible for reviewing this policy. The Trustees together with the GDPR Contact are responsible for monitoring this policy. This policy will be reviewed and updated when required or as detailed above.