Wheelchair Alliance

Community Interest Company

'Strengthening your voice'

Data Protection and Information Governance Policy

Issue date: **13th February 2023 (unanimous ratification at Board meeting)**

Review date: **12th February 2024 or following legislative change**

Approved by: **Nick Goldup (Chair and director)**

Jon Sawford (Company Secretary, Safeguarding lead & director)

Ray Hodgkinson (Honorary Treasurer and director)

Table of contents

1. Statement of intent

The Wheelchair Alliance is committed to protecting the rights and freedoms of individuals and safely and securely processing their data in accordance with all our legal obligations.

We hold personal data about our employees, volunteers, supporters, and other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data and ensure that our staff, volunteers and third parties understand the rules governing use of data they have access to for their work.

This policy requires consultation with the Wheelchair Alliance directors before any significant new data processing activity so that relevant compliance steps are addressed. Non-compliance may expose us to complaints, regulatory action, fines and/or reputational damage.

We are fully committed to ensuring continued and effective implementation of this policy and expect all staff, volunteers and third parties to share this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. Data Protection Principles

The Wheelchair Alliance will comply with the following data protection principles specified in the General Data Protection Regulation (GDPR):

1: *Lawfulness, Fairness and Transparency*

Data collection must be fair, for a legal purpose and be open and transparent as to how the data will be used.

2: *Purpose Limitation*

Data can only be collected for a specific purpose.

3: *Data Minimisation*

Any data collection must be necessary and not excessive for its purpose.

4: *Accuracy*

The data we hold must be accurate and kept up to date.

5: *Storage Limitation*

We cannot store data longer than necessary.

6: *Integrity and Confidentiality*

The data we hold must be kept safe and secure.

2.1 Accountability and transparency

We must ensure accountability and transparency in our use of personal data, and we must show how we comply with each Principle. A written record of how our data processing activities comply with each of the Principles must be kept. These must be kept up to date and approved by the director responsible for Compliance. We must show compliance with data protection law and the accountability and transparency Principle of the GDPR. Staff members and volunteers are expected to understand their responsibilities to ensure the Wheelchair Alliance meets the following data protection obligations:

• Complete all appropriate technical and organisational measures to protect an individual's data

• Maintain up to date and relevant documentation on all processing activities

• Conduct and document Data Protection Impact Assessments where appropriate

• Implement measures to ensure privacy by design and default, i.e. include privacy consideration from the start of a project when designing new systems or processes, including:

o Data minimisation – only capture data that is required, not what could be useful in the future

o Pseudonymisation – consider amending data in such a way that no individuals can be identified from the data without a “key” that allows data to be re-identified

o Transparency in how we are processing an individual’s data

o Creating and improving security and enhanced privacy procedures on an ongoing basis

3. Fair and Lawful Processing

Personal data must be processed fairly and lawfully. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

We must establish a lawful basis for processing data. At least one of the following must apply whenever we process personal data:

1. *Consent*

We hold recent, clear, explicit and defined consent for the individual's data to be processed for a specific purpose.

2. *Contract*

The processing is necessary to fulfil or prepare a contract for the individual.

3. *Legal obligation*

We have a legal obligation to process the data (excluding a contract).

4. *Vital interests*

Processing the data is necessary to protect a person's life or in a medical situation.

5. *Public Function*

The processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. *Legitimate interest*

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

3.1 Special categories of personal data

Previously known as sensitive personal data, this relates to data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to an individual's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

The special categories include information about an individual's:

- Race
- Ethnic origin
- Politics

• Religion

• Trade union membership

• Genetics

• Biometrics (where used for ID purposes)

• Health

• Sexual orientation.

In most cases where we process special categories of personal data, we will require the individual's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data, then that processing activity must cease.

3.2 Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. The Wheelchair Alliance cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such.

3.3 Children's and young person's data

Children need particular protection when we are collecting and processing their personal data because they may be less aware of the risks involved. If we are processing children's personal data, then we should think about the need to protect them from the start and design any systems and processes with this in mind. We will need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing but is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.

Our privacy notices need to be clear, and written in plain, age-appropriate language for children and their parents. We should gain consent from whoever holds parental responsibility. When we refer to a child, we mean anyone under the age of 18.

4. Our responsibilities

4.1 Wheelchair Alliance responsibilities

• Analysing and documenting the type of personal data we hold

• Checking procedures to ensure they cover all the rights of the individual

• Identifying the lawful basis for processing data

• Ensuring consent procedures are lawful

• Implementing and reviewing procedures to detect, report and investigate personal data breaches

• Storing and destroying data in safe and secure ways

• Assessing the risk that could be posed to individual rights and freedoms should data be compromised.

4.2 Volunteers, supporters and third-party responsibilities

• Fully understand your data protection obligations

• Check that any data processing activities you are dealing with comply with this policy and are justified

• Do not use data in any unlawful way

• Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions

• Comply with this policy at all times

• Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

4.3 Responsibilities of the Senior Information Risk Officer (SIRO)

The Company Secretary has responsibility for compliance within the Wheelchair Alliance and, as such, acts as the SIRO. Their responsibilities are:

• Keeping the board and directors team updated about data protection responsibilities, risks and issues. The board has overall responsibility for the Wheelchair Alliance compliance with data protection legislation

• Reviewing and approving all data protection procedures and policies on a regular basis

• Oversight of data protection training and advice for all staff members and those included in this policy

• Checking and approving data protection privacy notices used throughout the organisation

• Answering questions on data protection from staff, volunteers, board members and other stakeholder

- Responding to individuals such as people who wish to know which data on them we hold
- Ensuring all initiatives adhere to data protection laws and this policy.
- Ensuring all ICT systems, services, software and equipment have been assessed for security risks, agree actions to minimise and mitigate risk
- Ensuring that any identified mitigations are regularly reviewed and tested
- Ensuring any third-party ICT services used for storing and processing data meet our security requirements and obligations.

4.4 Accuracy and relevance

We must ensure that any personal data we processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We must not process personal data obtained for one purpose for any additional unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record that the accuracy is disputed and inform the Company Secretary.

4.5 Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Company Secretary will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

4.8 Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with our retention, archiving and destruction of information schedule.

4.9 Transferring data internationally

There are restrictions on international transfer of personal data. You must not transfer personal data abroad, or anywhere else outside of normal, approved business platforms without express permission from the Company Secretary.

5. Privacy Notices

A privacy notice (also known as 'fair processing information', 'privacy information', or a 'privacy policy') refers to information about why you need people's personal data, what you plan to do with it, how long you're going to keep it, and if you'll share it with anyone else.

Privacy notices must be concise, transparent, understandable, and easily accessible. They must be provided free of charge and written in clear and plain language. If they are aimed at children, they should be provided in an age-appropriate way.

A privacy notice must be supplied at the same time the data is obtained, if taken directly from the individual. If the data is not taken directly from the individual, a privacy notice must be provided within a reasonable period of having received the data, i.e. within one month.

If the data is being used to communicate with the individual, then the privacy notice should be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

6. Rights of Individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights:

Right to be informed

Right of access

Right to rectification

Right to erasure

Right to restrict processing

Right to data portability

Right to object

Rights in relation to automated decision making and profiling.

7. Third Parties

7.1 Using third party controllers and processors

As a data controller, we must have written contracts in place with any third-party data controllers and/or data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities. As a data controller, we must only appoint processors who can provide sufficient guarantees under the GDPR including that the rights of data subjects will be respected and protected. As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under the GDPR and we will protect and respect the rights of data subjects.

7.2 Contracts

Our contracts must comply with the standards set out by the Information Commissioners Office (ICO) and, where possible, follow the standard contractual clauses available. Our contracts with data controllers and/or data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify that:

• Acting only on written instructions

• Those involved in processing the data are subject to a duty of confidence

• Appropriate measures will be taken to ensure the security of the processing

• Sub-processors will only be engaged with the prior consent of the controller and under a written contract

• The controller will assist the processor in dealing with subject access requests and allow data subjects to exercise their rights under the GDPR

• The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments

• All personal data will be deleted or returned at the end of the contract

• Regular audits and inspections can be carried out and information submitted as necessary for the controller and processor to meet their legal obligations

• Nothing will be done by either the controller or processor to breach the GDPR

8. Data audit, monitoring and training

8.1 Data audits

We are committed to keeping an information audit up to date in order to manage and mitigate risks. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

8.2 Monitoring

Everyone must comply with this policy fully. We will keep this policy under review and amend or change it as required. The Honorary Secretary must be informed of any breaches of this policy.

8.3 Training

Staff and volunteers will receive adequate training on the GDPR and provisions of data protection law specific to their role. If additional training on data protection matters is identified, the Honorary Secretary should be informed.

9. Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. We have a legal obligation to report any material data breaches to the ICO within 72 hours. You have an obligation to report actual or potential data protection compliance failures i.e. 'near misses'.

This allows us to:

• Investigate the failure and take remedial steps if necessary

• Maintain a register of compliance failures

• Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures. Anyone who fails to notify a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the Wheelchair Alliance at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal/request to stand down as a volunteer. If you have any questions or concerns about anything in this policy, do not hesitate to contact the Honorary Secretary.

Policy Review

The Company Secretary will review this policy on an annual basis in conjunction with the directors, and will make any changes necessary

All Board members are required to familiarise themselves with this policy upon their appointment to the Board.