DATA PROTECTION POLICY

Version	2
Policy code	POL-07
Author	RiseHR/H Flack
Approved by	Steering Committee
Approval date	June 2023
Review date	June 2025

DATA PROTECTION POLICY

1. Policy Statement

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our members, suppliers and customers and any others we communicate with, and we recognise the need to treat it in an appropriate and lawful manner.

2. Purpose and Scope of the Policy

This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, customers, and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the EU General Data Protection Regulation (GDPR) and other UK data protection law. These laws impose restrictions on how we may use that information.

We have a commitment to ensuring that personal data is processed in line with GDPR and relevant UK law and that all our employees conduct themselves in line with this and other related policies. Where third parties process data on our behalf, we will ensure that the third party takes the necessary measures to maintain our commitment to protecting personal data.

This Data Protection Policy, also known as a Privacy Standard. Any breach of this policy will be taken seriously and may result in disciplinary action.

3. Who is covered by this policy?

This policy applies to all individuals working at all levels of the organisation, including senior managers, officers, trustees, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term workers, casual and agency staff and volunteers (collectively referred to as **staff** in this policy).

4. **Who is responsible for this policy?**

   The Steering Committee is responsible for ensuring compliance with GDPR and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to the Steering Committee.
   If you consider that this policy has not been followed in respect of personal data about yourself or others you should raise the matter with your manager or the Steering Committee.

5. **Definition of Data Protection terms**

   Data is personal information about an individual who can be directly or indirectly identified from that information. Data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). This personal information is referred to as 'Data' in the remainder of this policy.

   Data Subjects for the purpose of this policy include all living individuals about whom we hold Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Data.

   Data Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any Data is processed. They have a responsibility to establish practices and policies in line with relevant laws. We are the Data Controller of all Data used in our business.

   Data Users include members whose work involves using Data. Data Users have a duty to protect the Data they handle by following our data protection and security policies at all times. All members have a responsibility, when using Data, to comply with any security safeguards and procedures we put in place.

   Data Processors include any people who or organisations which process Data on behalf of a Data Controller. It could include third party suppliers which handle Data on our behalf.

   Processing is any activity that involves use of Data. It includes obtaining, recording or holding Data, or carrying out any operation or set of operations on Data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Data to third parties.

   Special Categories of Data are sensitive categories of Data about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, or

sexual orientation. It also includes genetic and biometric Data (where used for ID purposes). Special Categories of Data can only be processed under strict conditions and may require the explicit consent of the person concerned.

Criminal Offence Data is Data which relates to an individual's criminal convictions and offences. It can only be processed under strict conditions and may require the explicit consent of the person concerned.

Data Breach is any act or omission which compromises the security, confidentiality, integrity or availability of Data, or the safeguards that we or a third party put in place to protect the Data, including losing the Data or disclosing it to unauthorised people.

6. DATA PROTECTION PRINCIPLES

Anyone processing Data must comply with the eight enforceable principles of good practice. These provide that personal data must be:
Processed fairly, lawfully, and in a transparent manner. (Fairness, Lawfulness and Transparency)

- Processed for specified, explicit and legitimate purposes and in an appropriate way. (Purpose Limitation)

- Adequate, relevant and limited to what is necessary for the stated purpose. (Data Minimisation)

- Kept accurate and up to date (Accuracy)

- Not kept longer than necessary for the stated purpose. (Storage Limitation)

Processed in a manner that ensures appropriate security of Data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical or organisational measures. (Security, Integrity and Confidentiality)

Not transferred to another country without appropriate safeguards being in place. (Transfer Limitation)

Processed in line with Data Subjects' rights. (Data Subject's Rights and Requests)

We are responsible for and need to demonstrate compliance with the data protection principles listed above (Accountability).

a. Fairness and Lawfulness

   The purpose of GDPR and UK data protection laws is not to prevent the processing of Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the Company), who the Data Controller's representative is (in this case the Privacy Officer), the purpose for which the data is to be processed by us and the legal basis for doing so, and the identities of anyone to whom the Data may be disclosed or transferred.

   GDPR allows processing of Data for specific purposes, which are where it is needed:

   - for the performance of a contract, such as an employment contract
   - to comply with a legal obligation
   - in order to pursue our legitimate interests (or those of a third party) and where the interests and fundamental rights of the Data Subject do not override those interests
   - to protect the Data Subject's vital interests
   - in the public interest, or
   - in situations where the Data Subject has given explicit consent.

   We, as Data Controller, will only process Data on the basis of one or more of the lawful bases set out above. Where consent is required, it is only effective if freely given, specific, informed and unambiguous. The Data Subject must be able to withdraw consent easily at any time and any withdrawal will be promptly honoured.
   Special Categories of Data and Criminal Convictions Data will only be processed with explicit consent of the Data Subject, unless the Data Controller can rely on one or more of the other lawful bases set out above, and any additional legal bases for processing specific to these types of data, details of which have been set out in an appropriate Privacy Notice issued to the Data Subject.

b. Transparency

   We will provide all required, detailed and specific information to Data Subjects about the use of their Data through appropriate Privacy Notices

which will be concise, transparent, intelligible, easily accessible and in clear and plain language.

c. Purpose Limitation
Data may only be processed for the specific purposes notified to the Data Subject via the Privacy Notice. This means that Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the Data is processed, the Data Subject must be informed of the new purpose via a new or amended Privacy Notice before any processing occurs.

d. Data Minimisation
Data should only be collected to the extent that it is required for the specific purposes notified to the Data Subject in the Privacy Notice. Any Data which is not necessary for those purposes should not be collected in the first place.

e. Accuracy
Data must be accurate, complete and kept up to date. Information which is incorrect is not accurate and steps should therefore be taken to check the accuracy of any Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Data should be amended or destroyed.

i. Storage Limitation. Data should not be kept longer than is necessary to carry out the specified purposes. This means that Data should be destroyed or erased from our systems when it is no longer required, and in accordance with our Data Retention Policy.

ii. Security, integrity and confidentiality. We will ensure that appropriate technical and organisational security measures are taken against unlawful or unauthorised processing of Data, and against the accidental loss of, or damage to, Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

- We will put in place procedural and technological safeguards appropriate to our size, scope and business, our available resources and the amount of Data we hold, to maintain the security of all Data from the point of collection to the point of destruction.
- We will consider and use, where appropriate, the safeguards of encryption, anonymisation and pseudonymisation (replacing identifying information with artificial information so that the Data Subject cannot be

identified without the use of additional information which is kept separately and secure).

- We will regularly evaluate and test the effectiveness of these safeguards. Employees have a responsibility to comply with any safeguards we put in place.
- Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Data, defined as follows:
- Confidentiality means that only people who are authorised to use the Data can access it.
- Integrity means that Data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the Data if they need it for authorised purposes.

Failure to follow rules on data security may be dealt with via the Disciplinary Procedure.

iii. Data subjects rights and requests. Data must be processed in line with Data Subjects' rights. Data Subjects have the following rights which apply in certain circumstances:

- The right to be informed about processing of Data
- The right of access to their own Data
- The right for any inaccuracies to be corrected (rectification)
- The right to have information deleted (erasure)
- The right to restrict the processing of Data
- The right to portability
- The right to object to the inclusion of Data
- The right to regulate any automated decision-making and profiling of Data
- The right to withdraw consent when the only legal basis for processing Data is consent
- The right to be notified of a Data Breach which is likely to result in high risk to their rights and freedoms
- The right to make a complaint to the Information Commissioner's Office or other supervisory authority.

A formal request from a Data Subject for details of Data that we hold about them must be made in writing (Data Subject Access Request). Any member of staff who receives such a written request should forward it to their manager immediately. Please see the Subject Access Request Policy for full details.

iv. Automated processing (including profiling) and automated decision making (ADM). Specific further rules to protect Data Subjects apply to any Automated Processing (including Profiling) and ADM related to that person's Data. We may during the course of an employee's employment, or at the assessment stage of a recruitment activity request that an individual provide their explicit consent to carry out a Psychometric Test so that we can assess an employee's suitability for a role or increase awareness and knowledge of personal attributes that will best suit particularly roles or teams.

a. Direct Marketing. We are also subject to further rules and privacy laws about the processing of Data when marketing to our customers. You must comply with any separate guidelines we issue on direct marketing to customers.

b. Breach notification. Where a Data Breach is likely to result in a risk to the rights and freedoms of the individual(s) concerned, we will report it to the Information Commissioner's Office within 72 hours of us becoming aware of it, and it may be reported in more than one instalment.

Individuals will be informed directly if the breach is likely to result in a high risk to their rights and freedoms.

If the breach is sufficient to warrant notification to the public, we will do so without undue delay.

If you know or suspect that a Data Breach has occurred, do not attempt to investigate the matter yourself but contact your manager or the Data Privacy Officer immediately. You should preserve all evidence relating to the potential Data Breach. Please see the Data Breach policy for full details.

V. Training. New members must read and understand this policy as part of their induction. All members are to protect individuals' Data to which they have access, to ensure data security and to understand the consequences to themselves and us of any potential breaches of the provisions of this policy.

VI. Records. We will keep full and accurate records of all our data processing activities.

7. Policy review

This Policy will be reviewed at least every two years. The next formal review will therefore take place in June 2025. This Policy may be reviewed earlier should there be a legislative or other significant need.