CLEARVIEW
Movable Wall Solutions

Data Protection Policy

Clearview Movable Wall Solutions Limited
Unit 34 | Commerce Court | Challenge Way | Cutler Heights Lane | Bradford | BD4 8NW

INDEX

1. Policy Statement

This is the Data Protection Policy Statement of

Clearview Movable Wall Solutions Limited

Clearview Movable Wall Solutions Limited (Clearview) recognises its obligation to comply with GDPR and the Data Protection principles in the correct storage, disposal and other administration of any sensitive personal details it holds about its students, staff, suppliers and any other external agencies. In summary, it commits that all data held by Clearview will:

- Protect any data securely and it will only be used by Clearview for the service that we provide.
- Not sell data or give data to a third party without prior consent from the individual.
- Keep your personal information/data safe & private.
- Allow individuals to request access to any information/data that we may hold and if there are any mistakes we will correct it.
- Individuals may request for information/data to be removed or erased.

Robert Adams
Director

Date: 1st September 2024

Date of next review: 1st September 2025

2. Objective

The objective of this policy is to protect the personal information processed by or disclosed to staff or students of Clearview or other authorised persons (all hereinafter referred to as Data Owners and Data Users) ensuring its confidentiality, integrity and availability by processing it in accordance with current legislation.

3. Responsibilities of Staff, Students, suppliers and Authorised Third Parties

3.1 Managing Director

On behalf of Clearview, the Managing Director is responsible for approving the GDPR policy and for ensuring that it is discharged to all members of staff. The Managing Director is also responsible for appointing a Data Controller.

3.2 Data Owner

A Data Owner is responsible for:

- Informing the Data Controller when a new dataset has been established or if the use or purpose of data stored in a dataset, which has already been registered, has changed.
- Ensuring that the data is kept up-to-date and that amendments are made promptly following notification of changes.
- Ensuring that the security measures are appropriate for the types of personal data being processed.

3.3 Data Use

All staff, suppliers and authorised third parties when processing personal data about others, whether held manually or electronically, are responsible for working in compliance with the Data Protection principles.

3.4 Data Subject

As Data Subjects, all staff, suppliers and authorised third parties are responsible for:

- Ensuring that any personal information that they provide to Clearview in connection with their employment, registration or other contractual agreement is accurate.
- Informing Clearview of any changes to any personal information which they have provided, e.g. changes of address.
- Responding to requests to check the accuracy of the personal information held on them and processed by Clearview, details of which will be sent out from time to time, and informing Clearview of any errors or changes to be made.
- If staff, suppliers and any external third part organisation request access to any of the personal data held on file that they complete the appropriate request in writing.

4. Data Security

It is the responsibility of all staff, suppliers and any third parties authorised to access Clearviews personal data sets to ensure that those data, whether held electronically or manually, are kept securely and not disclosed unlawfully, in accordance with Clearviews Data Protection Policy.
Unauthorised disclosure will usually be treated as a disciplinary matter, and could be considered as constituting gross misconduct in some cases.

5. Subject Consent to Processing

Clearview will observe the conditions for processing personal information as laid down by the General Data Protection Regulation and with this policy It will be assumed that consent has been given by the Data Subject for his/her personal data to be used for the purposes advised at the point of collection of that data but, where the data is defined as sensitive personal data under the Act, explicit consent must be obtained from the Data Subject by the Data User before processing can proceed.

6. Rights of Access to Personal Information

Clearview respects the right of individuals to access and check the accuracy of any personal data that is being kept about them, either on computer or in a relevant filing system. Requests for the access of information held must be made to the Data Controller in writing.

7. Publication of Centre Information

It is Clearview's policy to make as much information public as possible and, in particular, the following type of information may be available to the public through Clearview's publications or otherwise by inspection:

- List of staff, their internal telephone numbers and Clearview e-mail addresses.
- Photographs of staff.
- Publications dataset.
- Academic qualifications and certifications.
- Job title and grade of staff.
- Research expertise of academic staff.

Any individual who has good reason for wishing details in these lists or categories or other personal data to remain confidential should contact The Data Controller.

8. Retention of Data

Personal data processed for any purpose shall not be kept for longer than is necessary for those purposes or as required to comply with other legislation. Personal information relating to students are suppliers will normally be kept on file for the duration of the contract specifications or archiving purposes as set out by government funded organisations.

9. Policy Awareness

A copy of the Policy Statement will be given to all new members of staff of Clearview and to newly-authorised third parties. All staff of Clearview and authorised third parties will be advised of the existence of this policy which will be posted on Clearview website, as will any subsequent revision of the policy. All staff and authorised third parties are to be familiar with and comply with the policy at all times.

10. Information/data held by Clearview

Clearview are responsible for ensuring that all personal data/information held either electronically or manually is accurate, if when processing data to a third party it is identified that the data is incorrect. Clearview must inform the Third Party in order that they can correct their records

11. Privacy Notice

All information/data held by Clearview regarding personal & sensitive data will be shared with various external agencies as appropriate.

Any Data Subject who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Data Controller.

12. Status of the Policy

This policy does not form part of a formal contract of employment, but it is a condition of employment that members of staff whether freelance, self-employed or temporary will abide by the rules and policies made by Clearview from time to time. Compliance with the Data Protection Regulation is the responsibility of all staff and authorised third parties. Any breach of the DPR may lead to disciplinary action being taken, access to Clearview information facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up initially with Clearview's Data Controller.

13. Individual Rights

At Clearview, all individuals have the right to access or have their data/information erased.

Any individual who wishes to have one of these rights actioned by do the following:

- Firstly, complete the request in writing.
- Once the appropriate request has been completed they pass it onto the Data Controller, who will have authorisation to carry out the request.
- The report that contains the data/information requested will be produced in a format that is suitable for the individual.
- A record will be kept with the following information – when the request was made, by whom the request was made and the date ad when the request was actioned including the date it was given to the individual
- Once the information/data has been submitted to the individual they will sign to say that it was received and date the document.
- If the request identified that the information was incorrect, the Data Controller will amend the information/data within 7 working days and the individual will be notified in writing that the change has been made.
- All individuals must give at least 28 days' notice to the Data controller when making any request for information/data. Failure to do this could result in a delay of providing the information/data or in some instances result in a disciplinary as failure to follow Clearview procedures.
- If Clearview refuses a request, we will inform the individual why and that they have the right to make a complaint to supervisory authority (referring to Clearview complaint procedure) who will deal with the complaint with one month of the request.

14. Data Breach

In the event of a breach of data/information, depending on the severity Clearview will carryout a full investigation of the breach, this will be done initially by the Data Controller, and, if the breach is considered to be serious (loss of substantial data or access to data without authorisation) then the investigation will be carried out by the Managing Director.