Privacy Policy

The overall aim of Creating New Horizons (known from this point on in the document as CNH)
know what is happening to their personal data and to protect this data under the law.

1. The objectives of the policy are to:

1.1. Create and implement sufficient security measures to keep personal data protected. CNH do not manage or collect Sensitive Personal Data and therefore this is not covered in the policy

1.2. Outline how CNH stores data, for what purpose and for the length of time it will be stored – including the management of data quality

1.3. Provide an outline of clients' 'Right to be Forgotten' and what this involves

1.4. Identify the steps taken in the event of a security breach

1.5. Outline the areas of the GDPR law where CNH will be legally required to disclose information

1.6. Offer reassurance through regular reviews of this policy and client feedback on the our approach to Data Protection by Design

2. Data Protection Policy

It is the policy of CNH to:

2.1. Use password protected computers and encrypted USB sticks to store data.

2.2. Inform individuals that all Profiles from third party companies including Insights Discovery Profiles, Mindflick and any other similar products profiling or diagnostic tools, if downloaded will be stored for a maximum period of 2 years. This will be done from the time of questionnaire completion. CNH may decide upon a Client Review they will destroy copies of profiles prior to this 2-year deadline – this may be as a result of a request by the client, a change in relationship or due to storage issues

2.3. Only use data for the purpose for which they were intended and that data will not be shared with third parties

2.4. Login information to any third party portals will be changed every three months, ensuring that any mobile security breaches are minimised.

2.5. All bank account information is protected for the period of time necessary to ensure business transactions have been completed or until the business relationship has ended and then destroyed from all mobile devices and any associated CNH business systems. This includes work carried out on behalf of CNH on a contract basis by third party companies and individuals.

2.6. All appropriate Wi-Fi security measures are taken including such areas as WEP encrypted routers, with regular password updates scheduled.

3. Individual Rights. Under the GDPR Legislation each contact has a number of rights, these are outlined fully on the Information Commissioners Office Website. CNH has prepared for these rights by:

3.1. Committing to ensure clients are aware of any changes to the way in which their data is being used

3.2. Allow Clients access to any data, which is stored about them or their employees in a way that it is convenient and transparent to them. This also includes their right to port any information held about them to take and use for themselves for different purposes

3.3. Allowing Clients an easy way to have their personal data erased and forgotten from any systems used by CNH. This includes the right to have their anonymised data relating to them deleted, and excluded from statistics, profiling and forecasting

3.4. Regularly reviewing the way in which we are using the personal or private details of our clients, ensuring that we are only collecting the right data and that it is absolutely necessary for the purpose for which it is being collected. However, we reserve the right to charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive and for the same purpose.

3.5. Information will be supplied within a month of request, or within 2 months for any complex requests. If we require 2 months, we will inform you as to the explicit reason for this extension of time.

3.6. CNH does not use any automated profiling systems for marketing purposes, and therefore it is not included within this document.
4. Confidentiality, Integrity and Availability: CNH does all it can to ensure the 'confidentiality, integrity and availability' of our systems and services and the personal data we process within them. However, In the event of a security breach e.g. theft of a computer, the loss of a laptop or a data grabbing malware, we will:
4.1. The data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
4.2. The data we hold is accurate and complete in relation to why you are processing it; and
4.3. The data remains accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, we will take all necessary steps to recover it and therefore prevent any damage or distress to the individuals concerned.
4.4. We will ensure a 'data security first' mind-set is used by CNH to minimise the risk of any breaches
4.5. CNH will also carry out regular reviews of their security measures to ensure they are appropriate and effective, as well as any necessary Risk Assessments for unusual or large data requests
4.6. Make sure access to data and premises is only given to those within the organisation, with the right level of responsibility and seniority. This includes access to the office premises even when set within a residential building
4.7. Hard copy personal information is shredded and disposed of in a secure manner
4.8. Mobile devices are password protected and tracked, using Apps such as 'Find My Phone' and will be reported to the police should there be a theft inside or outside the office premises
4.9. Any cloud computing systems such as Dropbox, Insights Online, ICloud and Accounting Systems have a password change every three months.
5. Legal Disclosure: In certain specific circumstances, CNH will be legally required to disclose personal data. In these circumstances, the legal obligation overrides any objection the individuals may have
5.1. By or under any UK enactment;
5.2. By any rule of common law; or

5.3. By an order of a court or tribunal in any jurisdiction.
6. Policy Reviews: This policy will be reviewed on a regular basis:
6.1. During the first year of GDPR every three months;
6.2. And after this period it will be reviewed annually;
6.3. If there is a significant change to the nature of the CNH business or work of a significantly different nature is carried on a 'one-off' basis, this policy will again be reviewed
6.4. The review will also consider
6.4.1. A Data Protection by Design approach so as not to collect or hold on to unnecessary data
6.4.2. A Data Impact Assessment to understand the full impact of collecting and holding the data and the level of risk associated with the activity.
7. If an approved code of conduct or certification scheme covering the training and development industry for which CNH processes data becomes available, we will consider working towards membership as a way of demonstrating that you comply.
8. Under Article 30 of the GDPR CNH will keep a record of any specific data processing activities.
9. The person responsible for GDPR is Steve Robinson