WayMakers Privacy Notice - How we use Client information

Why do we collect and use Client information?
WayMakers will record, process and keep personal information on you/ the Client in accordance with Article 9 – 'processing of special categories of personal data' under the GDPR - from May 2018.

We use this data to:

- Support the Client's learning
- Make assessments on the Client's development
- Safeguard the Clients in our care in accordance with relevant legislation
- Comply with Government legislation
- Assess the quality of our services

WayMakers collect, hold and share two kinds of records of Clients using our service.

Developmental records
These include:

- Developmental information collected prior to the Client starting our service
- A copy of the Client's Progress Check
- Observations in a setting, photographs, video clips, samples of work and developmental assessment records.
- A summary of the Client's profile report.

Personal records
These include:

- Personal details – including the information provided on the Client's registration form and any consent forms and characteristics such as ethnicity, language and nationality.
- Contractual matters – including the Client's days and times of attendance, a record of the Client's fees and/or funding entitlement, any records of fee reminders and/or disputes.
- Emergency contact details – including those people, other than parents/guardians with authorisation to collect the Client from a setting.
- Client's health and well-being – including discussions about every day matters regarding the health and well-being of the Client with the parent/guardian, records of accidents and medication records.
- Safeguarding and Client protection concerns – including records of all welfare and protection concerns and our resulting actions, meetings and telephone conversations about the Client and any information regarding a Looked After Client.
- Early support and SEN – including any focused intervention provided by a setting, a record of the Client's IEP and, where relevant, their EHCP.
- Correspondence and reports – including letters and emails to and from other agencies and any confidential reports relating to the specific Client.

Collecting information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing Clients' data
We ensure that access to Clients' files is restricted to Alex Kelly and those authorised to see them. Alex Kelly will be responsible for storage of WayMakers Clients' information.

We retain Clients' records for seven years after we have finished working with them, except records that relate to an accident or Client protection matter. These are kept until the Client reaches the age of 25 years.

Sharing information
The information that you provide to us, whether mandatory or voluntary, will be regarded as confidential. We do not share information about your Client with anyone without consent unless the law and our policies allow us to do so.

We routinely share information without consent with:
- schools, colleges and other educational provisions that the Client attends
- our local authority where required in relation to EHCP documentation
- the Department for Education (DfE) as part of statutory data collections.
- The Independent Schools Inspectorate.

We are obliged to share confidential information without authorisation from the person who provided it, or to whom it relates, when:
- there is evidence that the Client is suffering or is at risk of suffering significant harm.
- there is reasonable cause to believe that a Client may be suffering, or is at risk of suffering, significant harm
- it is to prevent significant harm arising to the Client, young people or adults, including the prevention, detection and prosecution of serious crime.

Further information regarding information sharing and confidentiality can be found in the attached policies.

Requesting access to your personal data
Under data protection legislation, parents/guardians, Clients and young people have the right to request access to information about them that we hold. Where a Client is too young to give 'informed consent' the parent is the 'subject' of the file and has a right to see the information held.

Clients' developmental records may be shared with parents/guardians and requests to access these will be discussed with Alex Kelly as part of the service.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress

- prevent processing for the purpose of direct marketing

- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you would like to discuss anything in this privacy notice, please contact Alex Kelly on alex@waymakers.co.uk
If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

WayMakers - Data Protection Breach Policy & Procedure

Policy Statement

WayMakers is committed to handling personal data in line with best practice and as such this Policy details the procedures to use when dealing with and responding to data protection breaches. This is to ensure that incidents are responded to promptly, risks are minimised, learning is identified, and remedial actions are implemented.

This document has been designed to help and encourage all employees to achieve and maintain expected standards of conduct. It applies to all employees and anyone else working for and with WayMakers, and its aim is to ensure consistent and responsible practice.

These procedures apply to all staff, suppliers, contractors, agency workers, volunteers, governors, parents or anyone else who may handle or have an interest in personal data on behalf of the organisation.

PURPOSE

The purpose of an incident response is to ensure that:

- Data breach events are detected, reported, categorised and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of disclosure
- Mitigation improvements are made is put in place to prevent recurrence
- Serious breaches can be reported to the Information Commissioner
- Lessons learnt are communicated to the organisation as appropriate and can work to prevent future incidents.

DATA PROTECTION BREACHES

A data protection breach occurs when personal data (which includes any information that allows an individual to be identified), is processed without authorisation, and which may result in its security being compromised. For the purposes of this policy, data protection breaches include both confirmed and suspected breaches.

This procedure is concerned with the management of such data protection breaches, which involves the detection and reporting of breaches as well as learning from the breach and implementing appropriate remedial actions.

Most commonly, data protection breaches occur as a result of human error, theft, unauthorised access, equipment failure, hacking or loss

Examples of common incidents are:

Type	**Example**
Technical	Data Corruption Malware Corrupt Code Hacking
Physical	Unescorted visitors in secure areas Break-ins to sites Thefts from secure sites Theft from unsecured vehicles/premises Loss in transit/post Loss/ Misplacing memory stick/flash drive confidential papers left on public transport
Other	Data Input errors Non-secure disposal of hardware or paperwork Unauthorised disclosures (including verbal)

When a data protection breach has been discovered, whatever the reason for the breach, the following procedure should be implemented.

DISCOVERY

All WayMakers staff are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach has been discovered, where possible, a Data Protection Breach Reporting Form should be completed to the fullest extent possible at that time, which provides full details concerning the breach.

Once a data protection breach has been reported, an initial assessment will be made concerning the content, quality of data involved and the potential impact and risk of the breach.

This is achieved by interviewing the key personnel involved in the breach and their line managers and collecting as much information as possible to determine how the breach occurred, what actions have been taken, whether outside agencies are involved and whether the data subjects have been notified

Not all data protection breaches will result in formal ICO Reporting action. Some will be false alarms or "near miss" events that do not cause immediate harm to individuals or the organisation. These should still be reported, as analysis of these instances will provide valuable process feedback and opportunity for continual improvement.

REPORTING

Following a discovery of a breach and the receipt of such a report, consideration will be made regarding whether the matter needs to be reported to the Information Commissioner's Office (ICO) and whether individuals who are potentially affected need to be informed.

Current legislation states that any data protection breaches (irrespective of their severity) should be reported to the ICO as soon as possible and no later than 72 hours after their discovery, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.

In addition to this, the individuals affected by the breach should be informed if the breach is likely to pose a high risk to them. The individuals should be informed of the nature of the data breach and the steps that you are taking to protect their data.

The incident should also be logged in the Data Protection Breach Register.

CONTAINMENT AND RECOVERY

As soon as possible after the discovery of an actual or suspected data protection breach, consideration should be given to: -

- whether the breach has been contained as far as possible and whether any further steps can be taken to contain the data from further loss;

- whether any steps can be taken to mitigate the impact and risk of the loss;

- whether anything can be done to recover the data.

INVESTIGATION

Following the initial discovery/reporting of an incident, an investigation should be initiated to understand the full facts regarding the data protection breach. The extent of the investigation will be a matter for the Company to decide and may simply involve the collation of documents, or may be involve interviewing staff involved in the breach, collecting witness statements, etc.

REMEDIAL ACTIONS

Once the full facts have been ascertained, and the investigation has been concluded, consideration will be given to the learnings from the breach and most importantly, what remedial actions the organisation needs to take to prevent a recurrence of the incident, this may include any appropriate disciplinary action for individuals implicated in the breach.

Actions should be documented on an action plan, which is reviewed on a regular basis thereafter to ensure that the actions have been carried out.

During and/or at the end of the completion of the investigation the Data Protection Breach Reporting Form and the Data Protection Breach Register will be updated to ensure that all the details of the events have been properly documented.