Privacy Notice – Digital Development Portrait (DDP)

Nurture International is a global company specialising in a Developmentally Led, Trauma Sensitive, Nurture Approach to educational settings. Nurture International have two websites which are www.nurtureinternational.co.uk and www.digitaldevelopmentalportrait.net

Nurture International is a registered limited company who also offers charitable works. Our registered number is 12627899.

We are registered with the Information Commissioner's Office Reference: ZB535912

This notice is designed to inform you how we process personal data This notice applies to subscribers to the Digital Development Portrait, administered by Nurture International.

Personal Data We May Collect

We may collect and process personal data about you a users of the DDP, as well as that of your student whose data you input into toolkit.. Personal data, or personally identifiable information, means any information about an individual from which that individual can be identified. It does not include data where the identity has been removed (anonymous data). We collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data:** includes first name, last name, username or similar identifier, title, and gender.
- **Contact Data**: includes billing address, delivery address, email address and telephone numbers.
- **Business Data**: includes your business address and company name.
- **Technical Data**: includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access the services of Nurture International and the Digital Developmental Portrait Website and the Nurture International Website.

- **Profile Data**: includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- **Usage Data:** includes information about how you use the Nurture International and Digital Developmental Portrait Website and Services, including the full Uniform Resource Locators (URL) clickstream to, through and from the Nurture International Website and Services (including date and time); products you viewed or searched for; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page and any phone number used to call our customer service number.

How Personal Data Is Collected

We use different methods to collect data from and about you including via:

- **Direct Interactions:** You may give us your Identity, Contact and Financial Data when you fill in forms or correspond with us by post, phone, email or otherwise. This includes personal data you provide when you register to use the Digital Developmental Portrait Website or our Services or contact us when you report a problem with the Digital Developmental Portrait Website.
- **Automated Technologies or Interactions**: As you interact with the Digital Developmental Portrait we automatically collect Technical Data about your device, browsing actions, patterns, Location Data and Usage Data. We collect this personal data by using cookies, server logs, web beacons, pixels, and similar technologies about your device, and your use of the site.

Submitting Personal Information on behalf of another person

To aid the functionality of the Digital Developmental Portrait you are required to provide mandatory details about learners. This may include individual factors such as SEND details and other identifiable information. As you are submitting this personal information on their behalf you confirm you have identified a valid lawful basis under data protection regulations for doing so.

Please note that the ownership of this data remains with the administering organisation. This means the organisation or individual that has been given access to the Digital Developmental Portrait. It is the responsibility of the administering organisation to ensure the information held within the Digital Developmental Portrait remains accurate, and personal data is deleted when the assessments are no longer required for the individual learner.

Legal Basis For Processing

We will only use your personal data when the law allows us to. Most commonly we will use your personal data in the following circumstances:

- To fulfil our contractual obligations to you.
- Where it is necessary for our legitimate business interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- To comply with a legal obligation.

To the extent we process your personal data for any other purposes, we ask for your consent in advance or require that our partners obtain such consent.

Uses Of Personal Data

Under the UK GDPR we require a lawful basis in order to process your data lawfully. We may process your personal data under more than one lawful basis depending on the specific purpose for which your data is being used.

We will not sell or rent your personal data to anyone. We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

Purpose/Activity	Lawful basis for processing
To manage our relationship with you which will include:	a. Performance of a contract b. Necessary to comply with a legal obligation.

• Notifying you about changes to our terms of service, this Privacy Notice or changes to the Digital Developmental Portrait. • Contacting you when your subscription is due for renewal	c. Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services).
To administer and protect our business (including troubleshooting, data analysis, testing, system maintenance, support, updates, reporting and hosting of data).	a. Necessary for our legitimate interests b. Necessary to comply with a legal obligation
To investigate research questions related to learner's mental health; wellbeing; social, emotional and behavioural difficulties; and the Digital Developmental Portrait. This is based on information provided into the toolkit on learners, such as name, SEND identifiers and other associated characteristics	a. Performance of a contract
To deliver relevant DDP Services content and advertisements to you and measure or understand the	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy).

effectiveness of the advertising we serve to you	

How we store your data

Once your data has been collected, we use reasonable and appropriate measures to ensure its security, including strict controls over who can access and process your data.

Nurture International uses Internet Service Providers and servers located within the UK, Iceland, Australia, and the European Economic Area (EEA). Nurture International shall ensure that your personal information will be held by those Internet Service Providers in compliance with the appropriate regulation.

We will process your data for the duration in which we have a subscription with the organisation. It is the responsibility of the contracting organisation to keep the information contained within the Digital Development Portrait up to date, and remove any information of learner which is no longer required. Once subscription is no longer active, we will retain information for a period of 12 months and all information will be permanently deleted.

Sharing Data

Nurture International will not rent or sell your personal information to other organisations for use by them in their own direct marketing activities. We use data processors who are third parties who provide elements of services for us. We have contracts in place with our data processors which means that they cannot do anything with your personal information unless we have instructed them to do it. When it is necessary for us to transfer your personal information outside of the UK this will only be done in accordance with the UK GDPR.

We will only disclose your personal information to third parties if we are under a duty to disclose or share your personal data in order to comply with any legal obligation; or to protect the rights, property, or safety of Nurture International, our

donors or others. This includes exchanging information with other companies and organisations for the purposes of fraud detection and protection.

Your Rights
Under data protection law, you have rights including:
Your right of access - You have the right to ask us for copies of your personal information.
Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.
Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.
Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances.
Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you. If you would like to exercise any of your rights, please contact alison@nurtureinternational.co.uk

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us via the following means:
Email: alison@nurtureinternational.co.uk
Postal Address:
Data Protection Officer
Nurture International
Barnston House,
Beacon Lane,
Heswall.
CH61 DEE

You can also complain to the ICO if you are unhappy with how we have used your data.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

Updates or changes to this notice

We reserve the right to make changes to this Privacy Notice. Each time you visit this site you should check this notice to check that no changes have been made to any sections that are important to you. Where appropriate, any changes may be notified to you by email.

This notice was last updated in March 2024

Data Protection

INTRODUCTION

Nurture International is committed to protecting the rights and freedoms of data subjects (natural persons) and the safe and secure processing of their personal data in accordance with Data Protection Legislation.

The Digital Developmental Portrait received information from educational settings that can be highly sensitive and information that supports the SEND graduated approach

Data Protection Legislation means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003, all the foregoing as amended from time to time, and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

Nurture International hold personal data about our employees, clients, suppliers and other individuals for variety of business purposes and we are committed to keeping safe the privacy and personal information inputted by our clients on behalf of themselves in our shop or their learners and schools' data via the Digital Developmental Portrait. (DDP) owned by Nurture International.

This policy sets out how we seek to protect personal data and ensure that our employees and non-employees such as Associate consultants, understand the rules governing their use of the personal data to which they have access during their work.

In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Nurture International's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all our employees and Associate consultants share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

This policy has been approved by Nurture International's Chief Executive Officers, Alison Grimshaw and Yvonne Monaghan.

DEFINITIONS

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes, Collating school's information for the Digital Developmental Portrait *Business purposes include the following:* *- Compliance with our legal, regulatory, and corporate governance obligations and good practice* *- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* *- Ensuring business policies are adhered to (such as policies covering email and internet use)* *- Gathering data from schools via the Digital Developmental Portrait to which schools are responsible for* *Collecting information on our website shop for posting goods bought and emailing members.* *- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking* *- Investigating complaints* *- Checking references, ensuring safe working practices, monitoring, and managing staff access to systems and facilities and staff absences, administration and assessments* *- Monitoring staff conduct, disciplinary matters* *- Marketing our business* *- Improving services*

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Personal data we gather may include: individuals' phone numbers, email addresses, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationalities, job titles, and CVs. For full information on the personal information we process, please see the relevant Privacy Notice.*
Special categories of personal data	Special categories of personal data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy. *Special categories of personal data we gather include: Information from Schools regarding learner data such as SEND categories.*

Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law, the controller may be provided for in law.
Data processor	'Data processor' means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioner's Office. (ICO).

SCOPE

This policy applies to all processing of personal data whether:

- wholly or partly by automated means (i.e. by computer, apps or other digital system), or
- by other means (i.e. paper records) that form part of filing system or are intended to form part of a filing system.

This policy applies to all staff and anyone else working on our behalf including contractors, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies such as those relating to Internet and email use. We may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being implemented.

Who is responsible for this policy?

As our Data Protection Officer (DPO), has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary. alison@nutureinternational.co.uk.

Nurture International is not responsible for any data protection issues relating to any educational setting that does not comply with Nurture International's privacy notice or Terms & Conditions. All users must agree with these before accessing the DDP.

PURPOSE

The purpose of this policy is to also provide guidance on the Data Protection Principles that apply when any personal data belonging to or provided by data subjects is collected, stored or transmitted.

It is therefore imperative that all employees, contractors, and vendors, comply with the 6 Data Protection Principles, summarised below.

Personal data should:

1) Be processed fairly, lawfully and transparently.
2) Be collected and processed only for specified, explicit and legitimate purposes.
3) Be adequate, relevant and limited to what is necessary for the purposes for which it is processed.
4) Be kept accurate and up to date. Any inaccurate data must be deleted or rectified without delay.
5) Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
6) Be processed in a manner that ensures security, using appropriate technical and organisational measures.

Accountability and transparency

We must ensure accountability and transparency in all our use of personal data.

Data Protection Legislation obliges all employees to take a proactive approach to data protection.

In order to encourage best practice and to avoid penalties from the Information Commissioner's Office (ICO), all employees are required to read this policy, to treat others' personal data with due care and consideration and to ensure that Nurture International is able to demonstrate compliance with data protection regulations.

Controlling vs. Processing data

Nurture International is classified as a data controller and data processor. We are a data controller of our employee HR data but also for client/customer data that we process as part of administering our Digital Developmental Portrait, (a tool to support educational professionals to identify and meet learners' developmental needs), along with Sales and Marketing functions.

As a Data Controller, we remain ultimately liable for all of our data processing activities complying with Data Protection Legislation. This means that we must take responsibility for the compliance of our Data Processors as well as our own actions.

As a Data Controller, we must:

- Demonstrate the highest level of compliance responsibility.
- Comply and demonstrate compliance with all Data Protection Principles as well as the other UK GDPR and Data Protection Act 2018 requirements.
- Co-operate fully with the ICO or other supervisory authority.
- Manage data breaches and Data Subjects' rights requests efficiently and within specified timeframes
- Pay the data protection registration fee

We are a data processor when Nurture International is contracted by Educational Professionals, agencies and authorities in third party organisations to offer a service to collate data on subjects and process their personal data. In doing so we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing without the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller.

As a data processor, we must:

- Not use a sub-processor without the written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority.
- Ensure the security of the personal data.
- Keep accurate records of processing activities.
- Notify the controller of any personal data breaches.
-

If you are in any doubt about how we handle data, contact the DPO for clarification.

Lawful basis for processing data

Where we are a data controller, we must process personal data lawfully in accordance with individuals' rights under data protection regulations. This means that we must establish a lawful basis for processing personal data.

Employees must therefore ensure that any personal data they are responsible for managing or working with has a written lawful basis approved by the DPO.

If we cannot apply a lawful basis, our processing does not conform to the first Principle and will be unlawful. Data subjects have the right to stop the processing of any personal data that has been unlawfully processed and have it erased.

At least one of the following conditions must apply whenever we process personal data:

1. **Consent**
   We hold recent, clear, explicit, and defined consent for the data subject's data to be processed for a specific purpose.
2. **Contract**
   Processing is necessary to fulfil or prepare a contract for the individual.
3. **Legal obligation**
   Processing is necessary to meet a legal obligation (excluding a contract).
4. **Vital interests**
   Processing is necessary to protect a person's life or in an urgent medical situation.
5. **Public function**
   Processing is necessary to carry out a public function, a task of public interest, or the function has a clear basis in law assigned to us.
6. **Legitimate interest**
   Processing is necessary for the business/organisation's 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.

Deciding which condition to rely on

If you are making an assessment of the lawful basis of processing, you must first establish that the processing is necessary to achieve your purpose. This means the processing must be a targeted, appropriate way of achieving a stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means that doesn't require the use of the personal data. You must also only use the minimum data required to achieve the purpose (e.g. don't use a full date of birth if an age or age range will do).

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions. All data processing must be reported to and recorded by the Data Protection Officer.

We ensure that individuals whose data is being processed by us on the website www.nurtureinternational.co.uk , either Clients signing up to either an online or Face to Face Nurture International Educational Programme, a workshop/group training, cluster group support or ordering a book, will have some personal detail taken

and stored to allow Nurture International to be able to deliver the course fully and maintain customer communication/support.

These clients have the right to contact us and request for their data to be deleted. Clients are informed of the lawful basis for processing their data, as well as the intended purpose.

Any intended changes to processing must be reported to the DPO, who will approve wording and include relevant information in Nurture International's overall Privacy Notice published on our website.

Schools have a responsibility to hold an assessment policy which informs parents what and how assessments are taking place, and this must include how the DDP is used and details of inputted data on their child.

SPECIAL CATEGORIES OF PERSONAL DATA

What are special categories of personal data?

Previously known as sensitive personal data, special category data is data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person'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 including political opinions and party support or membership.
- religion
- philosophy
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

Whenever we process special category data, we must identify a condition for processing as well as a lawful basis. The condition for processing special categories of personal data must comply with the law. If we cannot identify a condition for processing special categories of data, that processing activity must cease.

Nurture International processes special categories of personal data inputted from schools as part of their SEND categories). Within the personal data of the learners, ethnic origin, pupil premium, looked after status and SEND (Special Educational or Additional Educational Difficulties/Needs status are requested. Each educational professional who inputs information must have permission from the Headteacher or Head of Service.

Each user has an individual email and an individual password. Each educational professional can see the data that they have personally inputted. The admin user (Usually the Head teacher/Head of Service and those given permission by the Head teacher/Head of Service) can see the information collected and processed of all the learners in the school/service. It is up to the Headteacher/Head of Service who has permission to see the information collected and processed.

Criminal record checks

DBS and Safeguarding procedures.

All associates will have an advanced DBS to ensure safeguarding procedures can be followed.

Nurture International are committed to working effectively to keep children and adults alike safe and treated with respect and dignity.

Our safeguarding policy outlines how we meet our legal responsibilities and you can access this by contacting the safeguarding yvonne@www.nurtureinternational.co.uk

RESPONSIBILITES

Nurture International 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 data in safe and secure ways
- Assessing the risk that could be posed to individual rights and freedoms should data be compromised.

- Fully understand our data protection obligations
- Check that any data processing activities we are dealing with comply with our 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 the actions of others.
- 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.

Responsibilities of the Data Protection Officer/Manager

- Keeping the Patrons and key personnel updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreements regarding data processing.
- Monitoring compliance with data protection legislation across the organisation

Responsibilities of the Safeguarding Officer

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Check and scan security hardware and software regularly to ensure it is functioning properly.
- Research third-party services, such as cloud services the company is considering using to store or process data.
- Assist the DPO to deal with data protection queries from clients, target audiences or media outlets.

- Coordinate with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

If you aren't clear the purpose for which data was collected but wish to use it, or you wish to use it for another purpose, you must seek approval from the DPO who can confirm the purpose for which the data was collected and whether any proposed new purpose is compatible. Where the proposed use is significantly different, involves combining data from different sources, or otherwise might have a significant impact on data subjects, the DPO may require that a Data Protection Impact Assessment is undertaken.

Sometimes we use data for research purposes. This data is anonymised before public release to protect clients from identification.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data security

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

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.

- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
- The DPO must approve any cloud used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the company's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software.
- All possible technical measures must be put in place to keep data secure

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

If you are responsible for any data, you must consult with the DPO and ensure that an appropriate retention period is applied and the data included on the retention schedule. A copy of our Retention schedule can be obtained on request from the DPO.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO. Nurture International have separate servers for different countries outside of Europe, ensuring compliance with relevant data protection regulations.

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 in the following ways:

Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

Right of access (Subject Access Requests)

- Enable individuals to access their personal data and supplementary information.
- Allow individuals to be aware of and verify the lawfulness of the processing activities.

Right to rectification

- We must rectify or amend the personal data of an individual if requested because it is inaccurate or incomplete.

Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.

- We are permitted to store personal data if it has been restricted, but not process it further. We must retain just enough data to ensure the right to restriction is respected in the future.

Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services where we process it on the basis of consent or contractual obligation.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task unless there is an overriding reason to continue the processing.
- We must respect the right of an individual to object to direct marketing, including profiling and will cease if an objection is received.

- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

Rights in relation to automated decision making and profiling.

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

We must deal with rights requests without undue delay and within one calendar month. However, we may extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual. We must let the individual know within one month of receiving their request and explain why the extension is necessary.

DATA SUBJECT ACCESS REQUESTS

What is a data subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information, which means the information which should be provided in a privacy notice.

How we deal with data subject access requests?

- We must provide an individual with a copy of the information upon request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.
- If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.
- We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

- Once a data subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

RIGHT TO ERASURE

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws.
- To comply with a legal obligation
- The processing relates to a child.

How we deal with the right to erasure

We can refuse to comply with an erasure request where processing is necessary for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual; or
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

THIRD PARTIES

As a data controller (and data processor), we must have written contracts in place with any third party 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 data protection legislation that the rights of data subjects will be respected and protected, and the personal data will be kept secure.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under data protection legislation and we will protect and respect the rights of data subjects.

Contracts

Our contracts must comply with the minimum contractual requirements set out in the UK GDPR. Nurture International own the website and the Digital Developmental Portrait site. We pay the developer hosting payments monthly to ensure the security of data is compliant with UK GDPR and the system is working correctly for schools and individuals.

At a minimum, our Data Processing Agreement include terms that specify:

- The processor will act only on the requests from the controllers at Nurture International.
- 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 allowing data subjects to exercise their rights under Data Protection Legislation
- The processor will assist the controller in meeting its Data Protection Legislation obligations in relation to the security of processing, notification of data breaches and performance of Data Protection Impact Assessments
- The processor will delete or return all personal data at the end of the contract.
- The processor will submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.

- Nothing will be done by either the controller or processor to infringe Data Protection Legislation

If you are going to share data with another organisation, you must contact the DPO who can provide or advise on suitable wording. The agreement must be approved by the DPO.

AUDITS, MONITORING AND TRAINING

Data audits

Regular data audits to manage and mitigate risks will be carried out. This includes 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. You must conduct a regular data audit as required by the DPO and normal procedures.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. Nurture International will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy. You must comply with this policy fully and at all times.

Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities change, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the DPO.

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. For externally reportable breaches, Nurture International has a legal obligation to report the data breach to the ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. 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.

Any member of staff who fails to notify of 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.

Please refer to our Data Breach Policy and Procedure for more details.

COMPLIANCE

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.

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer.

Any individual who considers that the Policy has not been followed in respect of Personal Data about themselves should also raise the matter with the Data Protection Officer.

Further information about the DPA 2018 and the UK GDPR can be found on the Information Commissioner's Office (ICO) website: https://ico.org.uk/