General Data Protection Regulation

Date of Review: June 2019 Date of Next Review: June 2020

Version 3.0

This policy applies to all Stakeholders

Directors Approval:

Lewis Fogarty Ben Bausor

Key Documents:

- General Data Protection Regulation (2018)
- Data Protection Act (2018)
- Human Rights Act (1998)
- The Equality Act. (2010)

Terms used in this policy:

- 'The Academy' refers to any provision run by Always Growing Ltd or Always Growing Together CIC Limited
- 'Children' refers to any registered child or young person attending The Academy
- 'Staff' refers to all staff and volunteers
- 'Safeguarding team' refers to staff who have specific responsibilities for safeguarding
- 'Safeguarding' refers to the protecting children from maltreatment preventing impairment of children health and development, ensure the children have the provision of safe and effective care and taking action to enable all children to have the best outcomes.
- 'The Directors' refers to Lewis Fogarty and/or Ben Bausor or a nominated person who they have authorised to make decisions on their behalf.
- 'Parents' refers to parents, guardians, carers or anyone who has parental responsibility.

All policies are approved by the Directors of Always Growing Ltd and Directors of Always Growing Together CIC Limited, in line with the available guidance both Statutory and best practice. We envisage that these policies will apply to provision delivered by Always Growing Ltd or Always Growing Together CIC Limited. We review and update policies in a timely manner and endeavour to include statutory updates. In exceptional circumstances, for example a situation arising that is not covered by the policies below, the Directors will use their professional judgement to make the best possible decision in the circumstances. At all times, the Directors will keep in mind the needs and wishes of the child.

Contents

1. Aims

1.1 Always Growing aims to ensure that all personal data collected about staff, children, parents, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

1.2 This policy applies to all personal data (as per the definitions below), regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

2.1 This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: •Name (including initials) •Identification number •Location data •Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: •Racial or ethnic origin •Political opinions •Religious or philosophical beliefs •Genetics •Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes •Health – physical or mental •Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

4.1 Always Growing processes personal data relating to parents, children, staff, visitors and others, and therefore is a data controller.

4.2 Always Growing is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

5.1 This policy applies to **all staff** employed by Always Growing, and to external organisations or individuals working on our behalf, such as volunteers. Individuals who do not comply with this policy may face disciplinary action.

5.2 The Directors have overall responsibility for ensuring that Always Growing complies with all relevant data protection obligations.

5.3 The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

5.4 The DPO is also the first point of contact for individuals whose data Always Growing processes, and for the ICO.

Our DPO is Ben Bausor and is contactable via ben@alwaysgrowing.co.uk, 07917 885553 or 07761 293425

5.5 Staff are responsible for:

•Collecting, storing and processing any personal data in accordance with this policy

•Informing Always Growing of any changes to their personal data, such as a change of address or any other information that is relevant

•Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

6.1 The GDPR is based on data protection principles that Always Growing must comply with.

6.2 The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

6.3 This policy sets out how Always Growing aims to comply with these principles.

7. Collecting personal data

Lawfulness, fairness and transparency

7.1 We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Always Growing can **fulfil a contract** with the individual, or the individual has asked the Always Growing to take specific steps, such as providing a quote or information about Always Growing's services before entering into a contract
- The data needs to be processed so that Always Growing can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that Always Growing can perform a task **in the public interest,** and carry out its official functions in line with the statutory guidance and expectations placed on it
- The data needs to be processed for the **legitimate interests** of Always Growing or a third party (provided the individual's rights and freedoms are not overridden)

- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear **consent**

7.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

7.3 Further information about our lawful processing is outlined in the Appendix

7.4 Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

7.5 We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

7.6 If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

7.7 Staff must only process personal data where it is necessary in order to do their jobs, and must seek advice regarding personal information processing when they are unsure

7.8 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with Always Growing's Information and Records Policy.

8. Sharing personal data

8.1 We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this, but retain the right to not seek consent if it is deemed doing so would pose a risk or a delay in obtaining the consent would lead to an increased risk to an individual
- Our suppliers or contractors need data to enable us to provide services to our staff and children – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

8.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

8.3 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our children or staff.

8.4 Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

Subject access requests

9.1 Individuals have a right to make a 'subject access request' to gain access to personal information that Always Growing holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

9.2 Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

9.3 If staff receive a subject access request they must immediately forward it to the DPO.

Children and subject access requests

9.4 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

9.5 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children at Always Growing may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights

will always be judged on a case-by-case basis. The Directors reserve the right to seek further advice if required before granting requests.

9.6 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children at Always Growing may not be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis. The Directors reserve the right to seek further advice if required before granting requests.

Responding to subject access requests

9.7 When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

9.8 We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

9.9 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

9.10 A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

9.11 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

9.12 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest

- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

9.13 Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Photographs and videos

10.1 As part of Always Growing's activities, we may take photographs and record images of individuals within our setting.

10.2 We will obtain consent, as part of the booking and registration process from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the child.

10.3 Uses of photographs and evidence may include:

- On notice boards and in publications, brochures, newsletters, etc.
- Outside of Always Growing by external agencies such as in newspapers or part of marketing or information campaigns
- Online on our website or social media pages

10.4 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

10.5 When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

11. Data protection by design and default

11.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the Always Growing's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

12. Data security and storage of records

12.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

12.2 In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office or other desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the l office
- Passwords that are at least 8 characters long containing letters and numbers are used to access Always Growing computers, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Always Growing Staff, who store personal information on their personal devices are expected to follow the same security procedures as for Always Growing-owned equipment and will be provided with encryption software where necessary. Most data will be processed on Always Growing owned laptops
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

13. Disposal of records

13.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

13.2 For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Always Growing's behalf.

If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14. Personal data breaches

14.1 Always Growing will make all reasonable endeavours to ensure that there are no personal data breaches.

14.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

14.3 When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- Any non-anonymised information being published
- Safeguarding information being made available to an unauthorised person
- The theft of a laptop containing non-encrypted personal data

15. Training

15.1 All staff are provided with data protection training as part of their induction process.

15.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or Always Growing's processes make it necessary.

16. Monitoring arrangements

16.1 The DPO is responsible for monitoring and reviewing this policy.

16.2 This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed **annually** and reviewed with the Directors and Senior Leadership Team.

17. Links with other policies

17.1 This data protection policy is linked to our:

- Safeguarding Policy
- Equal opportunities policy
- Booking policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will discuss with the SLT
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored securely on Always Growing computer systems
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:

- ♣The categories and approximate number of individuals concerned
- ♣The categories and approximate number of personal data records concerned
- oThe name and contact details of the DPO
- oA description of the likely consequences of the personal data breach
- oA description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

oIf all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

oThe DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- oThe name and contact details of the DPO
- oA description of the likely consequences of the personal data breach
- oA description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

oThe DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

oThe DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- oFacts and cause
- oEffects
- oAction taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on Always Growing computer systems

•The DPO and SLT will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

•If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

•Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

•In any cases where the recall of email is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and

request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2: Lawful Basis for Processing Data

All data processing under GDPR must have a clearly identifiable lawful basis for processing. As part of Always Growing's commitment to GDPR, the following section outlines the lawful basis for processing that we have identified and how we have determined this.

Always Growing recognises that there may be situations where processing the data is covered by more than one legal basis

Any changes to these basis will be communicated and updated as our policy is reviewed, and all information processed will be necessary and proportionate.

1. Legal Obligation:

1.1 Always Growing is required to process personal data in order to comply with common law or statutory obligations that are placed on Always Growing as both an employer and a provider of childcare

1.2 There are a number of areas where Always Growing is required to process personal information to fulfil a statutory obligation. These are outlined below:

- Always Growing is registered with Ofsted and is compliant with the duties outlined in the EYFS Framework (2017) and needs to process personal data as part of our statutory responsibilities outlined in this framework, including liaison with Ofsted
- Always Growing has legal obligations to safeguard children and staff, as outlined in the EYFS Framework and Working Together to Safeguard Children and Keeping Children Safe in Education Documents
- To ensure the safety of all children in our care, Always Growing is required to process personal information for the purposes of establishing which children are on site at any one time or who are booked in that day/session or time period
- To safely collect children from school, Always Growing is required to process personal information and share with staff the names of children being collected from each school
- As an employer, Always Growing is required to liaise with HMRC for tax purposes
- All staff a required to have a valid DBS check and this may require Always Growing process personal data to ensure this can be carried out
- Keeping employees safe at work as outlined by legislation with health and safety
- Always Growing has duties under the Equality Act (2010) to promote equality

2. Fulfilling a Contract

1.1 Always Growing is required to process personal data in order to fulfil contracts that Always Growing as both an employer and as a provider of childcare

1.2 There are a number of circumstances where Always Growing will process information in order to fulfil a contract. These are outlined below:

- Always Growing needs to process personal data to comply with the obligations set out in the contract of providing childcare. This contract is made when the parent makes a booking for their child, and processing the name, date of birth and sensitive data is necessary in order to fulfil the contract
- Always Growing needs to process personal data to share with staff the children that they are aware of who they are collecting from each school, where this has been authorised, and ensure the that children can be collected safely
- Always Growing may process personal data in order to check payment has been made through Stripe, childcare vouchers and/or the government childcare voucher scheme
- Always Growing has employment contracts with the staff and volunteers working with Always Growing, and this requires the processing of personal data in order to pay employees
- Always Growing may be required to share personal data with suppliers so that they are able to provide a service that Always Growing has contracted them to provide for or on behalf of Always Growing. For example, sharing staff information with the payroll provider so staff can be paid. Capita process applications for DBS and this may require information being shared with them
- Always Growing has a staff appraisal process in line with our pay and progression policy. Personal date may be processed in terms of conducting this process successfully and sharing data with Managers and Directors so that the process can be completed

3. Vital Interests

3.1 Always Growing will process personal data in order to protect or save the life of another

3.2 There are a number of circumstances where Always Growing will process information in order to protect vital interests. These are outlined below:

- Always Growing may need to liaise with the emergency services in order to process personal data to protect someones life. This may be releasing health information or next of kin contact details in the event that the person is unable to give consent themselves
- Always Growing will need to process contact details for parents and medical or other needs for children to ensure that the information is available to pass to the emergency services to protect the individual when someone's life is at risk
- Always Growing will need to process medical and dietary information to ensure that the staff are aware of the needs of children in their care and can therefore take appropriate action to safely care for children attending Always Growing and protect their vital interests
- Always Growing may need to process medical information and next of kin information in order to ensure that the lives of staff can be protected in an emergency

4. Legitimate Interests

4.1 Always Growing may process personal data outside of the scope of the tasks required as a childcare provider. When processing data in this way, it will be in a way that:

- A person would reasonably expect
- Has a minimal privacy impact
- Has a compelling justification
- Does not infringe on the interests, rights or freedoms of the individuals

4.2 Always Growing would not anticipate using this lawful basis for tasks other than to inform parents or carers about Always Growing's services that are directly related to our provision as a childcare provider and ensure that parents have accurate, up to date information about Always Growing and the childcare provisions that we offer. This could include:

- Informing parents about changes to our policies and procedures
- Informing parents about bookings being available
- Keep parents updated about the childcare provision and support that Always Growing is able to offer

5. Public Task

5.1 Always Growing as a provider of childcare may process personal data in order to carry out a task in the public interest. Processing data in this way means that we are able to fulfil our statutory obligations set out in terms of the statutory requirements that are considered in the public interest

5.2As a registered provider of childcare, Always Growing is bound by the terms and conditions outlined in the EYFS handbook and relevant safeguarding legislation.

6. Consent

6.1 Always Growing anticipates being able to use the other bases for processing personal information, without the need for specifically obtaining consent to process information

6.2 Examples where Always Growing will seek consent may include:

- Sending marketing emails to parents
- Using photos and videos of children attending Always Growing
- Attending trips organised by Always Growing
- Administering medication on behalf of a parent