

# Data Protection Policy

*This policy aims to provide important direction and guidance on how we process personal data and share information that applies to all staff.*

Implemented: April 2021

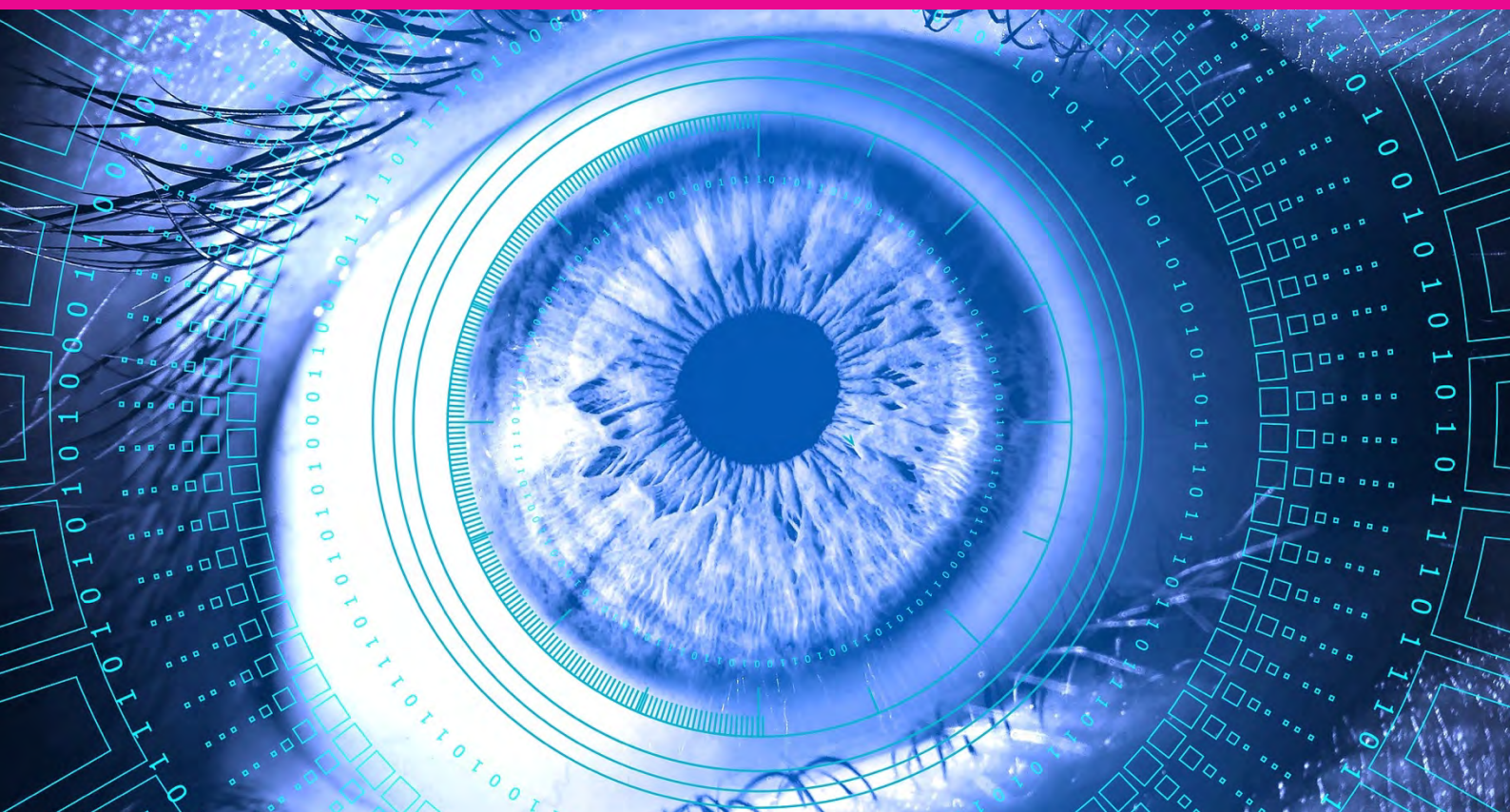
## Introduction

*This Data Protection policy aims to provide important direction and guidance on how we process personal data and share information that applies to all staff.*

Our approach to Data Protection is defined by the conditions of the General Data Protection Regulations (GDPR), applied from 25<sup>th</sup> May 2018.

## Contents

| SECTION    | TITLE   | PAGE |
|------------|---|------|
| ONE        | Introduction to Data Protection                         | 2    |
| TWO        | Information Sharing (Safeguarding)                      | 3    |
| THREE      | The Meaning of Key Data Protection Terms                | 4    |
| FOUR       | Summary of Data Protection Principles                   | 4    |
| FIVE       | Our Use of Data Protection and Our Purpose              | 5    |
| SIX        | Our Specific Data Protection Measures                   | 6    |
| SEVEN      | Data Protection Principles                              | 8    |
| EIGHT      | Data Subject Rights                                     | 10   |
| NINE       | Data Subject Access                                     | 12   |
| TEN        | Data Handling Subject Access Requests                   | 13   |
| ELEVEN     | Data Rectification of Personal Data                     | 13   |
| TWELVE     | Erasure of Personal Data                                | 14   |
| THIRTEEN   | Restriction of Personal Data Processing                 | 14   |
| FOURTEEN   | Data Portability  | 15   |
| FIFTEEN    | Objections to Data Processing                           | 15   |
| SIXTEEN    | Automated Decision-Making                               | 16   |
| SEVENTEEN  | Profiling   | 16   |
| EIGHTEEN   | Accountability  | 17   |
| NINETEEN   | Privacy Impact Assessments                              | 17   |
| TWENTY     | Operational Measures                                    | 18   |
| TWENTY-ONE | Transferring Personal Data to a Country Outside the EEA | 19   |
| TWENTY-TWO | Data Breach Notification                                | 20   |



## Section One: Introduction to Data Protection

Dimensions Care collects and uses personal information (“personal data”) about children, young people, staff, parents and other individuals who use our services. This information is gathered as is consistent with our duty as a responsible provider of regulated and unregulated social care. In addition, we may be required by law to collect, use and share certain information.

The General Data Protection Regulation (“the Regulation”) regulates the processing of personal data. It protects the rights and privacy of all living individuals (including children). Personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images, etc.), and may include facts or opinions about a person. All individuals who are the subject of personal data gathering have a general right of access to the personal data that relates to them.

### The Reason for this Policy

- People have legal rights with regard to the way their personal data is handled;
- In the course of our business activities we collect, store and process personal data about our service users, staff, suppliers and other third parties. Therefore, in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data;
- All people working in or with our business are obliged to comply with this policy when processing personal data.

## About this Policy

- This policy and any other documents referred to in it sets out the basis upon which we will process any personal data we collect from data subjects. For example, service users and business contacts, or that is provided to us by data subjects or other sources;
- It also sets out our obligations in relation to data protection under the General Data Protection Regulation (“GDPR”);
- This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data;
- The procedures and principles set out herein must be followed at all times by all staff, agents, contractors, or other parties working on behalf of the Company;
- We aim to ensure the correct, lawful, and fair handling of personal data and to respect legal rights.

## Section Two: Information Sharing (Safeguarding)

Dimensions Care Limited is a social care organisation. As a Data Controller, Dimensions holds highly sensitive personal data about children, young people and their families, as well as staff and contractors. This is essential to our business as a responsible provider of social care services, but moreover it is a critical part of keeping service users safe from potential or actual harm.

The personal data we use is processed in accordance with strict conditions of confidentiality. These conditions must be maintained at all times and staff are bound by a clearly defined Confidentiality Agreement. All staff must sign a Confidentiality Agreement and it must be retained within their staff file.

There are occasions where sensitive information must be shared with relevant authorities, and professionals.

### *Working Together to Safeguard Children (2018; 2020) is clear that:*

- Effective sharing of information between practitioners and local agencies is essential for early identification of need, assessment and service provision;
- Sharing information increases our capacity to take action to keep children and young people safe;
- Information sharing is also essential for the identification of patterns of behaviour when a child or young person has gone missing;
- Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children and young people, which must be the paramount concern;
- All practitioners should aim to gain consent to share information, but they should be mindful of situations where to do so would place a child or young person at increased risk of harm. Information may be shared without consent if a practitioner judges that there is good reason to do so, and that the sharing of information will enhance the safeguarding of a child or young person in a timely manner. When decisions are made to share information, practitioners should record who has been given the information and why.

*All colleagues are expected to make responsible and informed decisions about when and with whom to share information. If there is ever any doubt, management advice must be gained before the information is sent and/or the DPO should be informed.*

## Section Three: The Meaning of Key Data Protection Terms

- Data is information that is stored electronically, on a computer, or in certain paper-based filing systems;
- Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information;
- Personal Data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name or date of birth) or it can be an opinion about that person (i.e. actions and behaviour);
- Data Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes;
- Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

## Section Four: Summary of Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply.

*This means that all personal data must be subject to:*

- **(Lawfulness, Fairness and Transparency)** processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- **(Purpose Limitations)** collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.



All data must be processed in line with data subjects' rights, in particular the right to:

- 1) Request access to any data held about them by a Data Controller (see also Clause 15);
  - 2) Prevent the processing of their data for direct-marketing purposes;
  - 3) Ask to have inaccurate data amended (see also Clause 9);
  - 4) Prevent processing that is likely to cause damage or distress to themselves or anyone else.
- **(Data Minimisation)** adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
  - **(Accurate)** accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
  - **(Storage Limitations)** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
  - **(Integrity and Confidentiality)** data safeguarding – processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Transfers outside UK must not be transferred to people or organisations situated in countries without adequate protection.

## Section Five: Our Use of Data Protection and Our Purpose

*We collect, hold, and process the personal data referred to below:*

The following personal data may be collected, held, and processed by Dimensions Care Limited:

*Dimensions Care Limited collects and uses personal information ("personal data") about children, young people, staff, parents' and other individuals who use our services. This information is gathered as is consistent with our duty as a responsible provider of regulated and unregulated social care. In addition, we may be required by law to collect, use and share certain information.*

## Section Six: Our Specific Data Protection Measures

*When we are working with personal data, we take the following measures:*

- All emails containing personal data must be encrypted. Our email provider holds ISO/IEC 27001:2013. This is a standard for creating an Information Security Management System (ISMS). ISO 27001 is recognised as the “cornerstone” for any organisation that is “serious about combatting threats to information security, including cybercrime”; (See Appendix Two)
- Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded; An entry must be made in the Destruction Register (Note: A Destruction Register is available in the staff office at each service). Electronic copies should be deleted securely. This means:
  - a) (For Mac Users) select “Secure Empty Trash;”
  - b) (For Windows Users) Use a third-party wiping program, like ‘CCleaner’ or ‘Eraser’ (Eraser can also cleanse unallocated disk space).
- Personal data may be transmitted over secure networks only. Transmission over unsecured networks is not permitted in any circumstances and may result in disciplinary measures;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where Personal data is to be sent by facsimile, transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or send using First Class Recorded Special Delivery and marked as ‘Confidential’;
- No personal data may be shared informally and if a member of staff, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer (“DPO”). The Data Protection Officer is Wayne Price;
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

(Continued over)

- No personal data may be transferred to any staff, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the DPO. Note: The nature of our business means that Case files should be shared with staff to ensure that there is sufficient and appropriate knowledge of the child or young person's needs and presentation. This is to mitigate risk to all service users and relevant stakeholders;
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise [without the formal written approval of the DPO and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary. Please note: Staff with access to company mobile telephones must ensure that files are deleted in a timely and responsible way.
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Dimensions Care where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);
- All personal data stored electronically should be backed up no less than once a week, with backups stored on Dimensions Care SharePoint AND/OR at our operational Head Office. All backups should be encrypted and secure;
- All electronic copies of personal data should be stored securely using passwords and data encryption;
- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords;
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;
- Personal data is not used by Dimensions Care for marketing purposes, without the explicit authority of the data subject.



## Summary of Data Protection Measures

Dimensions Care aim to ensure that colleagues have robust information security in place. Colleagues have a duty to inform the DPO if there are any concerns about the security measures.

### *In addition, colleagues must:*

- Not use sub-processors without DPO consent, who will require full details of rationale and purpose;
- Co-operate with the relevant Data Protection Authorities in the event of an enquiry;
- Report data breaches to the DPO without delay;
- Keep records of all processing activities;
- Comply with EU trans-border data transfer rules;
- Maintain confidentiality regarding data subject's rights;
- Assist management in managing the consequences of data breaches;
- Not view CCTV recordings without the express permission of the data controller;
- Ensure that CCTV is only used for the purposes of detecting criminality;
- Ensure that CCTV recordings are held for no longer than 31 days, subject to any Police requirements following an incident. Retention times may vary depending upon the severity of the incident monitored;
- Delete or return all personal data at the request of management and/or following cessation of employment; and
- Inform the DPO if the processing instructions potentially infringe GDPR compliance.

## Section Seven: Data Protection Principles

### ONE: Lawfulness, Fairness and Transparency

The GDPR is not intended to prevent the processing of personal data. However, it does aim to ensure that the processing of personal data is done fairly and without adversely affecting the rights of the data subject. The processing of personal data is lawful, if one (or more) of the following applies:

- **(Consent)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- **(Contract)** processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- **(Legal Obligation)** processing is necessary for compliance with a legal obligation to which the Data Controller is subject;
- **(Protection)** processing is necessary to protect the vital interests of the data subject or of another natural person;

(Continued over)

- **(Public Interest)** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
- **(Legitimate Interests)** processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (or young person aged less than 18 chronological years).

## **TWO: Purpose Limitations**

Dimensions Care collects and processes the personal data set out in Section Five of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and can include data received from third parties.

Dimensions Care only processes personal data for the specific purposes set out in Section Four of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which Dimensions Care process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

## **THREE: Data Minimisation**

Dimensions Care will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Section Five, above.

## **FOUR: Accurate**

Dimensions Care shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter.

In addition, Managers are responsible for checking the continued accuracy of data. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

## **FIVE: Storage Limitations**

Dimensions Care shall not keep personal data for any longer than is necessary. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

### *Six: Secure Processing*

Dimensions Care shall seek to ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

#### *There will be:*

- An assessment of the risks posed to individual data subjects; and
- Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

## *Section Eight: Data Subject Rights*

### *The Rights of Data Subjects*

#### *The GDPR sets out the following rights applicable to data subjects:*

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights with respect to automated decision-making and profiling.

## Keeping Data Subjects Informed

The Company shall ensure that the following information is provided to every data subject when personal data is collected:

- Details of Dimensions Care (“the Company”) including, but not limited to, the identity of Wayne Price, its Data Protection Officer;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Section Four of this Policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Where the personal data is to be transferred to a third party that is located outside of the United Kingdom (the “UK”), details of that transfer, including but not limited to the safeguards in place;
- Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);
- Details of the data subject’s rights under the GDPR;
- Details of the data subject’s right to withdraw their consent to the Company’s processing of their personal data at any time;
- Details of the data subject’s right to complain to the Information Commissioner’s Office (the ‘supervisory authority’ under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection/processing of the personal data and details of any consequences of failing to provide it;
- Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences;
- The information set out above shall be provided to the data subject at the following applicable time:
  - a) Where the personal data is obtained from the data subject directly, at the time of collection;
  - b) Where the personal data is not obtained from the data subject directly (i.e. from another party):
  - c) If the personal data is used to communicate with the data subject, at the time of the first communication; or
  - d) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
  - e) In any event, not more than one month after the time at which the Company obtains the personal data.



## Section Nine: Data Subject Access Requests

*A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them.*

Dimensions Care Limited is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

All subject access requests received must be forwarded to Wayne Price, the Company's data protection officer. Wayne may be contacted via email: [wayne@dimensionscare.co.uk](mailto:wayne@dimensionscare.co.uk) or by telephone: 07904 488050.

Dimensions does not charge a fee for the handling of normal SARs. However, we reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

All data subjects have a right of access to their own personal data, as defined by the Data Protection Act.

In order to ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Where a request for subject access is received from a child, we expect that:

- Requests from children will be processed as any subject access request. This is outlined on Page 13, and the copy will be given directly to the child, unless it is clear that the child does not understand the nature of the request or there are legal conditions prohibiting such action;
- Requests from children who do not appear to understand the nature of the request will be referred to those with parental responsibility;
- Requests from parents will be duly processed subject to any restrictive legal conditions.



**Data Protection: Subject Access Request (SAR) Form**

This subject access request (SAR) form can be used to make a request by or on behalf of an individual who is entitled to ask for under Section 45 of the Data Protection Act

Enquirer's Full Name: \_\_\_\_\_

Enquirer's Full Address: (Inc. Postcode) \_\_\_\_\_

Home Telephone: \_\_\_\_\_

Business Telephone: \_\_\_\_\_

Mobile Telephone: \_\_\_\_\_

Email: \_\_\_\_\_

Are you the person who is the subject of the records you are enquiring about? Please select either 'YES' or 'NO'

Do you have legal parental responsibility for a child who is the subject of the records you are enquiring about? Please select 'YES' or 'NO'

Name of child about whose personal data records you are enquiring about: \_\_\_\_\_

Please provide a brief description of the records you are enquiring about: \_\_\_\_\_

### Section Ten: Data Handling Subject Access Requests

*Requests must be made in writing. Children, parents or staff may ask for a Subject Access Request form (Above). Provided there is sufficient information to process the request, staff must record:*

- The date of receipt of request;
- The data subject's name;
- The name and address of requester;
- The type of data required (e.g. Child's case file, personnel record); and
- The planned date of supplying the information (normally not more than 40 days from the request date), should the request be considered appropriate.

Please note: Should more information be required to establish the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date upon which information has been provided.

### Section Eleven: Data Rectification of Personal Data

*If a data subject informs Dimensions Care Limited that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified.*

The data subject will be informed of that rectification within one month of receipt the data subject's notice. (N.B. this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

*In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.*

In addition, a notification may be sent to the Information Commissioner's Office (ICO), with whom Juventas are registered. This will be decided upon a case-by-case basis, ensuring that the threshold or notification is met. The threshold is based upon risk to people. This means whether or not people's rights and freedoms have been compromised following the breach.

The ICO are clear that we do not need to report every breach. If in any doubt, colleagues and other relevant stakeholders should speak with the DPO.



### Section Twelve: Erasure of Personal Data

*Data subjects may request that Dimensions Care Limited erases the personal data it holds about them in the following circumstances:*

- It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the Company holding and processing their personal data, depending upon any legal conditions regarding the service user and compliance regarding service user case file retention;
- The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so);
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

Unless Dimensions Care have reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with. The data subject informed of the erasure, within one month of receipt of the data subject's request. (N.B. This can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

### Section Thirteen: Restriction of Personal Data Processing

Data subjects may request that Dimensions Care Limited ceases processing the personal data it holds about them. If a data subject makes such a request, Dimensions shall retain only the amount of personal data pertaining to that data subject that is necessary (in accordance with our legal obligations to hold and share certain information) to ensure that no further processing of their personal data takes place.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

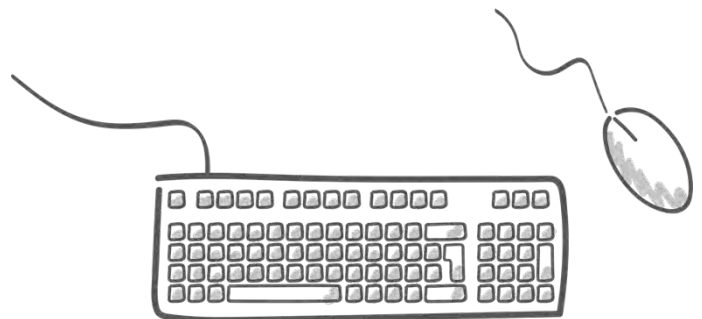
### Section Fourteen: Data Portability

*Dimensions Care Limited do not use automated individual decision-making software.*

Dimensions Care Limited do not use personal data for automated individual decision-making (i.e., making a decision solely by automated means without any human involvement)

Dimensions Care Limited do not use automated personal data profiling (i.e., automated processing of personal data to evaluate certain things about an individual).

The personal data of service users and, in exceptional circumstances, staff will only be sent to another Data Controller with an implicit legal basis that can be described as a “legitimate need.” For example, personal data relating to placement planning information and risk assessments, needs analysis well other matters relating to operating a responsible Social Care business.



### Section Fifteen: Objections to Data Processing

*Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.*

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

A data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.

Where a data subject objects to the Dimensions Care processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

## Section Sixteen: Automated Decision-Making

*Dimensions Care Limited does not use automated individual decision-making software.*

## Section Seventeen: Profiling

*Where the Company uses personal data for profiling purposes, the following shall apply:*

- Clear information explaining any profiling will be provided, including its significance and the likely consequences;
- Appropriate mathematical or statistical procedures will be used;
- Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
- All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

*Dimensions Care Limited is clear that profiling will only be used for the following:*

- Strategic development, specifically regarding regular analysis of the needs of service users and commissioning authorities. This will be an internal process and any data generated will be anonymised and maintained within the organisation. The information gathered will likely document anonymised service user's presenting factors and associated safety risks;
- Matching and impact assessments of placement referrals, specifically profiling the safety and presentation needs of those accommodated against those referred. This is an internal process and a further measure towards our commitment to safeguarding (i.e., Service user welfare).

*Dimensions Care Limited is clear that profiling will not be used for the following:*

- Marketing (including advertising and publicity materials).

*To comply with GDPR, Dimensions Care Limited:*

- Have a lawful basis to carry out profiling (that is documented in this policy);
- Only collect a minimum amount of data needed and have a clear retention policy (that is documented in this policy).

## Section Eighteen: Accountability

### Dimensions Care Limited's Data Protection Officer (DPO) is:

Mr. Wayne Price

Dimensions Care Limited  
5 Brooklands Place, Brooklands Road, Sale  
Cheshire, M33 3SD

e: wayne@dimensionscare.co.uk  
m: 07904 488050

Our ICO Registration Number is: ZA859408

### Accountability Statement:

Dimensions Care Limited shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Company, its data protection officer, and any applicable third-party Data Controllers;
- The purposes for which the Company processes personal data;
- Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;
- Details (and categories) of any third parties that will receive personal data from the Company;
- Details of any transfers of personal data to non-EEA countries including all security safeguards;
- Details of how long personal data will be retained by the Company; and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

## Section Nineteen: Privacy Impact Assessments

Dimensions Care shall carry out Privacy Impact Assessments as required under the GDPR. Privacy Impact Assessments shall be overseen by the Company's DPO and shall address the following areas of importance:

- The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
- Details of the legitimate interests being pursued by the Company;
- An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.

## Section Twenty: Operational Measures

*Dimensions Care Limited shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:*




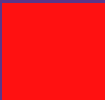
- All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- Methods of collecting, holding and processing personal data shall be regularly reviewed;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy;
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as defined by this Policy and the GDPR;
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

### Section Twenty-One: Transferring Personal Data to a Country Outside the UK

The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

#### Clarification of the European Economic Area (EEA)

|   |  |
|---|--|
|    | EU states which form part of the EEA   |
|   | EFTA states which form part of the EEA   |
|  | EU state which forms part of the EEA through the provisional application of an accession agreement |
|  | EFTA state which signed the EEA agreement but did not join   |



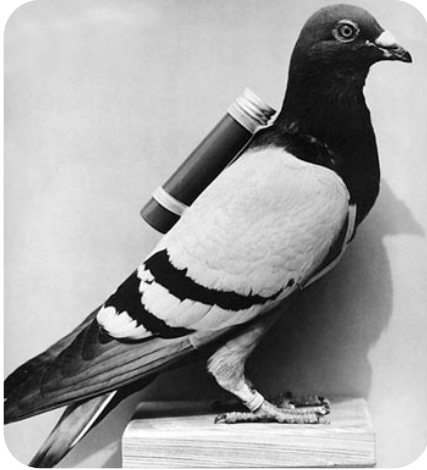
You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;
- Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- The transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.



## Section Twenty-Two: Data Breach Notification

*All personal data breaches must be reported immediately to the DPO.*



If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPO must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours.

In the event that a personal data breach is likely to result in a high risk (to the rights and freedoms of data subjects), the DPO must ensure that all affected data subjects are informed of the breach directly and without delay.

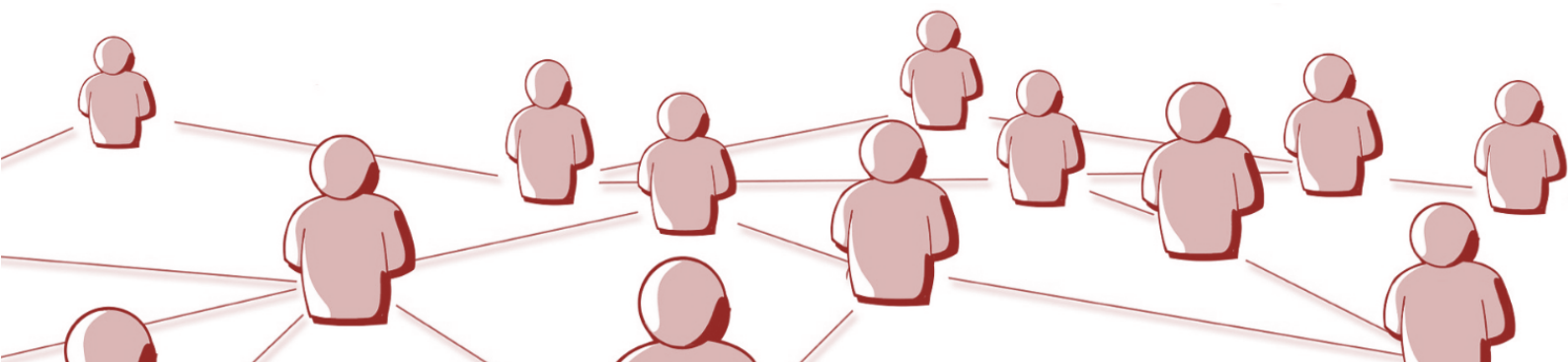
*Data breach notifications shall include the following information:*

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the DPO (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by Juventas Services Limited to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

## Section Twenty-Three: Implementation of This Policy

*This Policy shall be deemed effective as of 1<sup>st</sup> April 2021.*

This policy will be reviewed every 24 months, but amendments may be made in response to any relevant legislative changes within the interim period.



## The Quality Standards

### Regulation 5 Engaging with The Wider System to Ensure Each Child's Needs Are Met

The Quality Standards set out in regulations the outcomes that children must be supported to achieve while living in children's homes. Each standard has an aspirational, child-focused outcome statement, followed by a clear set of underpinning, measurable requirements that homes must meet to achieve the standard.

### *Engaging with the wider system to ensure children's needs are met*

5. In meeting the quality standards, the registered person must, and must ensure that staff—

- a) Seek to involve each child's placing authority effectively in the child's care, in accordance with the child's relevant plans;
- b) Seek to secure the input and services required to meet each child's needs;
- c) If the registered person considers, or staff consider, a placing authority's or a relevant person's performance or response to be inadequate in relation to their role, challenge the placing authority or the relevant person to seek to ensure that each child's needs are met in accordance with the child's relevant plans; and
- d) Seek to develop and maintain effective professional relationships with such persons, bodies or organisations as the registered person considers appropriate having regard to the range of needs of children for whom it is intended that the children's home is to provide care and accommodation.

### *The regulations prescribe nine Quality Standards for children's homes:*

- 1) The Quality and Purpose of Care Standard (Regulation 6)
- 2) The Children's Wishes and Feelings Standard (Regulation 7)
- 3) The Education Standard (Regulation 8)
- 4) The Enjoyment and Achievement Standard (Regulation 9)
- 5) The Health and Well-Being Standard (Regulation 10)
- 6) The Positive Relationships Standard (Regulation 11)
- 7) The Protection of Children Standard (Regulation 12)
- 8) The Leadership and Management Standard (Regulation 13)
- 9) The Care Planning Standard (Regulation 14)

## Google Security Audits and Certifications

At Google, ensuring the security of our users is a top priority, and we are constantly assessing how we can make our services even more secure. Google regularly undergoes independent verification of security, privacy and compliance controls. This means an independent auditor examines the controls present in our data centers, infrastructure and operations. These audits and certifications by accredited third-party auditors help verify the data protection technologies and processes Google is using, and show our commitment to protecting user data.

Among the certifications that Google Apps for Work, Google Drive for Work (Google Apps Unlimited) and Google Apps for Education have achieved are ISO 27001, ISO 27018, SOC 2 and SOC 3. In this paper we will provide additional details about those certifications and audits.



Auditors: EY CertifyPoint

### International Standards Organization (ISO) 27001 Certification

International Standards Organization (ISO) 27001 Certification is a widely recognized, internationally accepted independent security standard. Google's ISO 27001:2013 certification covers the systems, applications, people, technology, processes and data centers supporting Google Apps for Work and Google Apps for Education editions. Google's compliance with the ISO 27001 standard was certified by EY CertifyPoint, an ISO certification body accredited by the Dutch Accreditation Council, a member of the International Accreditation Forum (IAF). Certificates issued by EY CertifyPoint are recognized as valid certificates in all countries with an IAF membership.<sup>1</sup>

The ISO 27001 certification is composed of 114 controls. Highlights of Google's certification include certifying:

- Information security policies
- Physical and environmental security
- Organization of information security
- Operations security
- Asset management
- Logical security
- Access control
- Incident management
- Cryptography

**Issue Date:** April 15, 2015

### International Standards Organization (ISO) 27018

ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in a public cloud computing environment. The standard provides further implementation guidance on 14 of the 114 controls in ISO 27002 and contains 25 additional controls specifically focused on the processing of PII.

EY has verified Google's assertion that the privacy practices and contractual commitments for Google Apps for Work and Google Apps for Education meet the objectives defined by ISO/IEC 27018:2014.

**Issue Date:** July 15, 2015

<sup>1</sup> IAF Member Countries.



Auditors: EY LLP

## SOC 2 Type II and SOC 3 Audits

A Service Organization Control (SOC) report has a predefined set of principles and related criteria that are defined by American Institute of Certified Public Accountants (AICPA) and must be met to achieve an unqualified report. The criteria for SOC 2 are widely recognized. The [SOC 3 report](#) asserts publicly that Google Apps for Work is in conformity with the AICPA criteria for security, availability, process integrity and confidentiality.

EY issued an unqualified opinion with zero exceptions on any control objectives or control activities during the period covered for the report for Google Apps for Work, Google Drive for Work (Google Apps Unlimited) and Google Apps for Education.

The principles covered in the reports include:

- Security: The system is protected against unauthorized access (physical and logical).
- Availability: The system has mechanisms to prevent or quickly correct any service outages, including redundant sites that are in place for business continuity and backup and recovery of customer data.
- Processing Integrity: The system performs as you expect it to. Data is preserved to be the way you left it the last time you logged on.
- Confidentiality: The system has controls so data that is stored in the cloud is shared with only the people you wish to share it with.

Major control objectives and control activities covered by the audit include the following:

- Logical security controls provide reasonable assurance that logical access to production systems is restricted to authorized individuals.
- Data center physical security controls provide reasonable assurance that Google data centers and corporate offices are protected.
- Incident management controls provide reasonable assurance that problems and/or incidents are properly responded to, recorded, investigated and resolved.
- Change management controls provide reasonable assurance that application and configuration changes are tracked, approved, tested and validated.
- Organization and administration controls provide reasonable assurance that management provides the infrastructure and mechanisms to track and communicate initiatives, monitor compliance within the company and provide security training for the risks that impact Google.
- System availability controls provide reasonable assurance that redundant sites are in place for services and recovery of customer data is possible.

**Time period covered:** 1 May 2014 to 30 April 2015<sup>2</sup>

**Updated:** September 2015

<sup>2</sup> Due to the nature of SOC, these audits will always reflect a time frame that has passed. Audit reports measure point-in-time controls, so though the audit date may be in the past, this audit is current and has not expired.

**Google Apps for Work and Google Apps for Education security audits and certification summary.**

| Products and Services Covered           |  |  |  |
|---|--|---|---|
| Google Drive                            | ●  | ●   | ●   |
| Google Hangouts                         | ●  | ●   | ●   |
| Gmail                                   | ●  | ●   | ●   |
| Google Calendar                         | ●  | ●   | ●   |
| Google Docs                             | ●  | ●   | ●   |
| Google Sheets                           | ●  | ●   | ●   |
| Google Slides                           | ●  | ●   | ●   |
| Google Apps Vault                       | ●  | ●   | ●   |
| Google Sites                            | ●  | ●   | ●   |
| Google Admin console <sup>3</sup>       | ●  | ●   | ●   |
| Google Contacts                         | ●  | ●   | ●   |
| Google Apps Script                      | ●  | ●   | ●   |
| Google+                                 | ●  | ●   | ●   |
| Google Now                              | ●  | ●   | ●   |
| Google Groups                           | ●  | ●   | ●   |
| Google Talk                             | ●  | ●   | ●   |
| Google Classroom (Google for Education) | ●  | ●   | ●   |
| Apps Script Directory API <sup>4</sup>  | ●  | ●   | ●   |
| Reports API <sup>5</sup>                | ●  | ●   | ●   |
| SAML Based SSO API                      | ●  | ●   | ●   |

<sup>3</sup> Formerly Control Panel

<sup>4</sup> Formerly Directory Sync, and Provisioning API

<sup>5</sup> Formerly Reporting API, and Audit API





**Dimensions Care Limited**  
Registered in England and Wales under  
Company Number: 12205346

ICO Registration Number: ZA859408

**Dimensions Care Limited** © March 2021