Data Protection Policy

Author: David Helyer
Date: 5th June 2025
Review Date: 4th June 2026

Table of Contents

Scope of Policy

This Policy sets out the obligations of Attentive Care Solutions Ltd regarding data protection and the rights of children and young people, parents/carers, staff and visitors ('data subjects') in respect of their personal data under the Data Protection Act 2018 and the associated UK GDPR, including any subsequent amendments.

UK GDPR defines 'personal data' as any information relating to an identified or identifiable natural person (a '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.

This Policy sets out Attentive Care Solutions Ltd obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by Attentive Care Solutions Ltd, its employees, volunteers, contractors, or other parties working on behalf of Attentive Care Solutions Ltd.

Attentive Care Solutions Ltd. is committed not only to the letter of the law, but also the spirit of the law, and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and the Company Attentive Care Solutions Ltd. of all individuals with whom it deals.

This Policy is to be used, and understood, in conjunction with the Company ***Data Protection Procedures***, ***Photography Code of Conduct and Consent Form***, ***Complaints and Compliments Policy***, ***Allegations Policy***, ***Privacy Notice for Staff*** *and* ***Privacy Notice for Service Users****; see these*

documents for how Attentive Care Solutions Ltd. handles the data of staff and the children and young people who access our alternative education provision.

The Data Protection Principles

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

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit, and legitimate purpose 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 incompatible with the initial purpose.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. 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 it is processed, is erased, or rectified without delay.
5. Kept in a form that 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 UK GDPR in order to safeguard the rights and freedoms of the data subject.
6. 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.

The Rights of Data Subjects

The Data Protection Act 2018 and UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this Policy indicated for further details):

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure (also known as the 'right to be forgotten').
5. The right to restrict processing.

6. The right to data portability.
7. The right to object.
8. Rights with respect to automated decision-making and profiling.

Lawful, Fair, and Transparent Data Processing

UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. UK GDPR states that the processing of personal data shall be lawful if at least one of the following applies:

1. The data subject has given consent to the processing of their personal data for one or more specific purposes
2. The 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 with them
3. The processing is necessary for compliance with a legal obligation to which the data controller is subject
4. The processing is necessary to protect the vital interests of the data subject or of another natural person
5. The 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
6. The 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 that require protection of personal data, in particular where the data subject is a child.

If the personal data in question is 'special category data' (also known as 'sensitive personal data'), for example data concerning the data subject's race, politics, ethnicity, religion, trade union membership, genetics, biometrics (if used for identification purposes), health, sex life, or sexual orientation, at least one of the following conditions must be met:

1. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless UK law prohibits them from doing so)
2. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by UK law, which provides appropriate safeguards for the fundamental rights and interests of the data subject)
3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
4. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is

carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes, and that the personal data is not disclosed outside the body without the consent of the data subjects

5. The processing relates to personal data that is clearly made public by the data subject
6. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity
7. The processing is necessary for substantial public interest reasons, on the basis of UK law, which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject
8. The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of UK law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of UK GDPR
9. The processing is necessary for public interest reasons in the area of public health, for example protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of UK law, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy)
10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of UK GDPR based on UK law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Specified, Explicit, and Legitimate Purposes

The Company collects and processes the personal data set out in the section Personal Data Collected, Held, and Processed below. This includes:

1. Personal data collected directly from data subjects.
2. Personal data obtained from third parties.

The Company only collects, processes, and holds personal data for the specific purposes set out in the section Personal Data Collected, Held, and Processed in this Policy (or for other purposes expressly permitted by UK GDPR).

Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Refer to section Keeping Data Subjects Informed below for more information on how the Company carries this out.

Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data, and to the extent necessary, for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under section Specified, Explicit, and Legitimate Purposes above, and set out in Personal Data Collected, Held, and Processed below.

Accuracy of Data and Keeping Data Up to Date

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in the section Rectification of Personal Data below.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out of date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details on the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to the Data Retention Policy, which is available to all staff, and only on request to all service users.

Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures that shall be taken are provided in sections Data Security – Transferring Personal Data and Communications to Organisational Measures below.

Accountability and Record Keeping

1. Overall responsibility for data protection is managed by the Company Data Protection Lead: David Helyer Director
   info@attentivecaresolutions.co.uk

   who may use the services of external organisations when required.

2. The Data Protection Lead shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with UK GDPR and other applicable data protection legislation.
3. The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
   a. The name and details of the Company and any applicable third-party data processors.
   b. The purposes for which the Company collects, holds, and processes personal data.
   c. 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.
   d. Details of any transfers of personal data to non-European Economic Area (EEA) countries, including all mechanisms and security safeguards.
   e. Details of how long personal data will be retained by the Company (please refer to the Data Retention Policy).
   f. Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Data Protection Impact Assessments

1. The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data that involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under UK GDPR.
2. Data Protection Impact Assessments shall be overseen by the Data Protection Lead and shall address the following:
   a. The type(s) of personal data that will be collected, held, and processed.
   b. The purpose(s) for which personal data is to be used.
   c. The Company's objectives.
   d. How personal data is to be used.
   e. The parties (internal and/or external) who are to be consulted.
   f. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.
   g. Risks posed to data subjects.

h. Risks posed both within and to the Company.
i. Proposed measures to minimise and handle identified risks.

Keeping Data Subjects Informed

1. The Company shall provide the information set out in part 2. of this section below to every data subject:
    a. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection.
    b. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
        - If the personal data is used to communicate with the data subject, when the first communication is made
        - If the personal data is to be transferred to another party, before that transfer is made
        - As soon as reasonably possible, and in any event not more than one month after the personal data is obtained.
2. The following information shall be provided:
    a. Details of the Company, including, but not limited to, the identity of the Data Protection Lead.
    b. The purpose(s) for which the personal data is being collected and will be processed (as detailed in section Personal Data Collected, Held, and Processed below) and the legal basis justifying that collection and processing.
    c. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data.
    d. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.
    e. Where the personal data is to be transferred to one or more third parties, details of those parties.
    f. Where the personal data is to be transferred to a third party that is located in a territory without an adequacy agreement as approved by the UK Government, details of that transfer, including but not limited to the safeguards in place (see section Transferring Personal Data to a Country without an Adequacy Decision below) for further details.
        - *As a general rule, the Company does not transfer data outside the EEA. If this changes, employees will be notified of this and the protections that are in place to protect the security of employees' data will be explained. This will be done so in line with the **Data Protection Policy** and **Data Protection Procedures** and UK GDPR.*
    g. Details of data retention.
    h. Details of the data subject's rights under UK GDPR.

i. Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time.
j. Details of the data subject's right to complain to the Information Commissioner's Office (ICO) (the 'supervisory authority' under UK GDPR).
k. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.
l. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Data Subject Access

- Data subjects may make subject access requests ('SARs') at any time to find out more about the personal data the Company holds about them, what the Company is doing with that personal data, and why.
- Employees wishing to make a SAR should contact the Data Protection Lead.
- Responses to SARs shall normally be made within one month of receipt. However, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- Responses to SARs shall be dependent upon the terms of UK GDPR, the Data Protection Act (2018) and associated ICO guidance.
- The Company does not charge a fee for the handling of normal SARs. The Company reserves 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.

Rectification of Personal Data

- Data subjects may have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
- Where such rectification is possible, the Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

1. It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed
2. The data subject wishes to withdraw their consent to the Company holding and processing their personal data
3. 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; see section Objections to Personal Data Processing below for further details concerning the right to object)
4. The personal data has been processed unlawfully
5. The personal data needs to be erased for the Company to comply with a particular legal obligation

Unless the Company has reasonable ground to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's 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).

Restriction of Personal Data Processing

- Data subjects may request that the Company restricts processing the personal data the Company holds about them. If a data subject makes such a request, the Company shall, in so far as is possible, ensure that the personal data is only stored and not processed in any other fashion.
- If the Company is required to process the data for statutory purposes or for reasons of legal compliance, then the Company shall inform the data subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.
- 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).

Data Portability

1. The Company processes personal data using automated means. Such processing is carried out by Email, Cloud based, encrypted services and paper copy
2. Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely, transmitting it to other data controllers).
3. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
4. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

Objections to Personal Data Processing

- Data subjects have the right to object to the Company processing their personal data based on performing a task in the public interest, the Company's legitimate interests, or direct marketing (including profiling).
- Where a data subject objects to the Company processing their personal data, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
- Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.
- Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under UK GDPR, '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.

Automated Decision Making

1. The Company is not currently using personal data in automated decision-making processes. In the event that this situation changes, the Company shall notify data subjects of our intentions to commence such processing.
2. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge such decisions under UK

GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

3. The right described in point 2. does not apply in the following circumstances:
    a. The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject
    b. The decision is authorised by law
    c. The data subject has given their explicit consent.

Profiling

The Company uses personal data for profiling purposes. These purposes relate to helping YP accessing the Company's services to maximise their achievement and monitor staff performance.

When personal data is used for profiling purposes, the following shall apply:

1. Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling.
2. Appropriate mathematical or statistical procedures shall be used.
3. Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected.
4. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see sections Data Security – Transferring Personal Data and Communications to Data Security – IT Security for more details on data security).

Personal Data Collected, Held, and Processed

The Company uses a wide range of personal data across many processes. More detail can be found in the Company Data Protection Procedures, Privacy Notice for Service Users and Privacy Notice for Staff. If an employee or service user wishes to view the complete list of categories of personal data the Company processes, please contact the Data Protection Lead.

Data Security – Transferring Personal Data and Communications

The Company shall ensure that the appropriate measures are taken with respect to all communications and other transfers involving personal data:

- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

- The Company will ensure that, where special category personal data or other sensitive information is sent in the post, it shall be possible to demonstrate that the information was delivered.
- Where personal information is to be sent by facsimile transmission (including fax machines, and scanned and emailed documents), the recipient should be informed in advance of the transmission and should be waiting by the fax machine/for the email to arrive in their inbox to receive the data.
- Where special category personal data or other sensitive information is to be sent by email, the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document and not in the body of the email.
- Where personal data is to be transferred in removable storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by the Company.

Data Security – Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

1. All electronic copies of personal data should be stored securely using passwords, user access rights and, where appropriate, data encryption.
2. 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.
3. All personal data relating to the operations of the Company, stored electronically, should be backed up on a regular basis.
4. Where any member of staff stores personal data on a mobile device (whether that be a computer, tablet, phone, or any other device), then that member of staff must abide by the Acceptable ICT Use Policy. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information.

Data Security – Disposal

When 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 erased and disposed of. For further information on the erasure and disposal of personal data, see the Company Data Retention Policy.

Data Security – Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

1. No personal data may be shared informally and if an employee, volunteer, 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 Lead.
2. No personal data may be transferred to any employees, volunteers, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the initial authorisation of the Data Protection Lead.
3. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, volunteers, sub-contractors, or other parties at any time.
4. 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.
5. Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Data Protection Lead to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the Telephone Preference Scheme (TPS).

Data Security – IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

1. The Company requires that any passwords used to access personal data shall have a minimum of 8 characters, composed of a mixture of upper and lower case characters, numbers and symbols. Passwords are not expected to be changed on a regular basis, but users will be expected to change their password if instructed by the Company.
2. Under no circumstances should any passwords be written down or shared between any employees, volunteers, contractors, or other parties working on behalf of the Company, irrespective of seniority or department, **unless permission has been given by the Data Protection Lead**. If a password is forgotten, it must be reset using the applicable method. The IT support team do not have access to passwords.
3. All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Company's outsourced IT support team shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so.

4. No software may be installed on any Company owned computer or device without the prior approval of the Data Protection Lead.
5. Where members of staff or other users use online applications that require the use of personal data, the use of that application must be signed off by the Data Protection Lead.

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

1. All employees, volunteers, 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 UK GDPR, and under this Policy, and shall have free access to a copy of this Policy.
2. Only employees, volunteers, 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.
3. All employees, volunteers, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
4. All employees, volunteers, contractors, or other parties working on behalf of the Company handing personal data will be appropriately supervised.
5. All employees, volunteers, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.
6. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
7. All personal data held by the Company shall be reviewed periodically, as set out in the Data Retention Policy.
8. The performance of those employees, volunteers, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
9. The contravention of these rules will be treated as a disciplinary matter.
10. All employees, volunteers, 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 UK GDPR and this Policy by contract.
11. All 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 those relevant employees of the Company arising out of this Policy and UK GDPR.
12. Where any 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 that may arise out of that failure.

Transferring Personal Data to a Country without An Adequacy Decision

The Company does not send personal data outside the European Economic Area (EEA). If this changes, the relevant parties will be notified of this and the protections that are in place to protect the security of this data will be explained.

In such cases that the Company does transfer ('transfer' includes making available remotely) personal data to countries without a suitable adequacy decision from the UK Government, the following will apply:

1. The transfer of personal data to a country without an adequacy decision shall take place only if one or more of the following applies:
    a. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK Government has determined ensures an adequate level of protection for personal data
    b. The transfer is to a country (or international organisation) that provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK Government; compliance with a code of conduct approved by a supervisory authority (e.g. the ICO); certification under an approved certification mechanism (as provided for in UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority
    c. The transfer is made with the informed consent of the relevant data subject(s)
    d. The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject)
    e. The transfer is necessary for important public interest reasons
    f. The transfer is necessary for the conduct of legal claims
    g. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent
    h. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

A data breach is defined as: lack of confidentiality, availability, or fidelity (also called 'integrity') of information, whether stored or conveyed (to someone) by the Company.

1. All personal data breaches must be reported immediately to the Company, to the Data Protection Lead: David Helyer, Company Director Info@Attentivecaresolutions.co.uk
2. 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 Data Protection Lead must ensure that the ICO is informed of the breach without delay, and, in any event, within 72 hours after having become aware of it.
3. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under point 2.) to the rights and freedoms of (a) data subject(s), the Data Protection Lead must ensure that all affected data subjects are informed of the breach directly and without undue delay.
4. Data breach notifications shall include the following information:
    a. The categories and approximate number of data subjects concerned.
    b. The categories and approximate number of personal data records concerned.
    c. The name and contact details of the Company's Data Protection Lead (or other contact point where more information can be obtained).
    d. The likely consequences of the breach.
    e. Details of the measures taken, or proposed to be taken, by the Company to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of Policy

This Policy shall be deemed effective from the date of its authorship, given at the beginning of this document. No part of this Policy shall have a retroactive effect and shall thus apply only to matters occurring on or after this date.

The Data Protection Lead is responsible for the active and continued adherence to the implementation of this Policy, and of any subsequent updates to this Policy. Employees will be required to read this Policy and are responsible for the active and continued implementation of this Policy, and any subsequent updates to it, both by themselves and their colleagues.

If anyone has any queries, concerns, etc. regarding data protection at the Company, they are to contact the Data Protection Lead:

David Helyer,
Company
Director,
info@attentivecaresolutions.co.uk