Data Protection Policy

Document number: PP/ACG/IG01 Version 1

For the latest version of this policy please refer to the electronic location below or the website

Summary	In order to provide the service that it delivers and comply with regulatory and contractual requirements, Active Care Group (ACG) must process certain types of personal and sensitive data. In doing so ACG are therefore required to comply with data protection legislation. This includes in particular the Data Protection Act 2018 and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their *personal data* whilst imposing certain obligations on the ACG in order to process their data.
Scope	All Staff
Document Type	Policy ☒ SOP ☐ Guideline ☐
Verified by	Information Governance Steering Group
Version Issued	May 2019
Next Review Date	May 2022
Author	Quality and Governance Manager
Lead Director	Director of Governance and Quality
Electronic Location (EL)	Information Centre
Located on Website	Yes

Contents

1. Introduction

1.1. All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act 2018 and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their *personal data* whilst imposing certain obligations on the organisations that process their data.

1.2. As a healthcare provider and an employer ACG collects and processes both *personal data* and *sensitive personal data* relating to service users, customer related data, workers and temporary workers (for the purpose of this policy referred to as staff). It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

1.3. This policy sets out how ACG implements the Data Protection Laws.

2. Scope

2.1. This Policy applies to all directly and indirectly employed staff responsible for collecting and processing data within ACG and other persons working within the organisation.

2.2. This policy should be read in conjunction with ACG information governance and data protection policies, key legislative and regulatory requirements as well as division or service specific policies and procedures.

3. Definitions

3.1. **'*consent*'** means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of personal data relating to him or her;

3.2. **'*data controller*'** means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*;

3.3. **'*data processor*'** means an individual or organisation which processes *personal data* on behalf of the *data controller*;

3.4. **'*personal data*'*** means any information relating to an individual who can be identified, such as by 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.

3.5. **'*personal data breach*'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*;

3.6. **'*profiling*'** means any form of automated *processing* of *personal data* consisting of the use of *personal data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

3.7. **'*pseudonymisation*'** means the *processing* of *personal data* in such a manner that the *personal data* can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable individual;

3.8. **'*sensitive personal data*'*** means *personal data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

3.9. * For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we specifically need to refer to *sensitive personal data*.

3.10. **'*Supervisory authority*'** means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

4. Purpose for Processing Data

4.1. ACG processes *personal data* in relation to its own staff, work-seekers, individual service user contacts as well as customer related data and is a *data controller* for the purposes of the Data Protection Laws.

4.2. ACG may hold *personal data* on individuals for the following purposes:

- Administration and *processing* of work-seekers' *personal data* for the purposes of providing employment with ACG, including *processing* using website links and forms and back office support.
- Administration and processing of potential service users' *personal and sensitive data* for the purposes of providing a quote for a package of care. This data is shared with the funding third-party or service user directly depending on who is initiating the contract.
- Administration and processing of service users' *personal and sensitive data* for the purposes of producing a personalised plan of care and risk assessment for staff to follow, whilst complying with regulatory requirements
- Administration and *processing* of service users' *personal data* for the purposes of introducing staff.
- Allow us to ensure that we comply with the requirements of the third parties that we carry out business with.
- To comply with any legal requirements, pursue our legitimate interests and to protect our legal position.
- Staff administration.
- Accounts and records.
- Advertising, marketing and public relations (please refer to privacy policy on the website)

5. The Data Protection Principles

5.1. The Data Protection Laws require ACG acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and kept up to date; every reasonable step must be taken to ensure that *personal data* that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept for no longer than is necessary for the purposes for which the *personal data* are processed;
- 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; and that
- The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

6. Legal Bases for processing

6.1. ACG will only process *personal data* where it has a legal basis for doing so. Where the company does not have a legal reason for *processing personal data* any processing will be a breach of the Data Protection Laws.

6.2. ACG will review the *personal data* it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date

6.3. Before transferring *personal data* to any third party (such as past, current or prospective employers, suppliers, customers and service users, persons making an enquiry or complaint and any other third party (such as software providers and back office support), ACG will establish that it has a legal reason for making the transfer.

7. Privacy by Design and Default

7.1. ACG has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities. This includes implementing measures such as:

- Data minimisation (i.e. not keeping data for longer than is necessary);
- *pseudonymisation*;
- Anonymization;
- Cyber security.

For further information please refer to the Company's Information Security Policy.

8. Privacy

8.1. ACG shall provide any information relating to data *processing* to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. ACG may provide this information orally if requested to do so by the individual.

9. Privacy Notices

9.1. Where ACG collects *personal data* from the individual, the company will give the individual a privacy notice at the time when it first obtains the *personal data*.

9.2. Where ACG collects *personal data* other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the *personal data*, but

at the latest within one month. If the company intends to disclose the *personal data* to a third party then the privacy notice will be issued when the *personal data* are first disclosed (if not issued sooner).

9.3. Where ACG intends to further process the *personal data* for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further *processing*.

10. Subject Access Requests

10.1. The individual is entitled to access their *personal data* on request from the *data controller*. Requests can be made by contacting those listed in the appendix and responses will be received no longer than one month after the request was made where possible. See Subject Access Request Policy for full details.

11. Rectification

11.1. The individual or another *data controller* at the individual's request, has the right to ask ACG to rectify any inaccurate or incomplete *personal data* concerning an individual.

11.2. If ACG has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the *personal data* unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however ACG will not be in a position to audit those third parties to ensure that the rectification has occurred.

12. Erasure

12.1. The individual or another *data controller* at the individual's request, has the right to ask ACG to erase an individual's *personal data.*

12.2. If the company receives a request to erase it will ask the individual if s/he wants his *personal data* to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by ACG should the company come into possession of the individual's *personal data* at a later date.

12.3. If ACG has made the data public, it shall take reasonable steps to inform other *data controllers* and *data processors processing* the *personal data* to erase the *personal data*, taking into account available technology and the cost of implementation.

12.4. If ACG has given the *personal data* to any third parties it will tell those third parties that it has received a request to erase the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however ACG will not be in a position to audit those third parties to ensure that the rectification has occurred.

13. Restricting of Processing

13.1. The individual or a *data controller* at the individual's request, has the right to ask ACG to restrict its *processing* of an individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes its erasure;
- ACG no longer needs the *personal data* for the purposes of the *processing*, but the *personal data* is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the company override those of the individual.

13.2. If ACG has given the *personal data* to any third parties it will tell those third parties that it has received a request to restrict the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold –

however ACG will not be in a position to audit those third parties to ensure that the rectification has occurred.

14. Data Portability

14.1. The individual shall have the right to receive *personal data* concerning him or her, which he or she has provided to ACG, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *data controller* in circumstances where:

- The *processing* is based on the individual's *consent* or a contract; and
- The *processing* is carried out by automated means.

14.2. Where feasible, the Company will send the *personal data* to a named third party on the individual's request.

15. Object to Processing

15.1. The individual has the right to object to their *personal data* being processed based on a public interest or a legitimate interest. The individual will also be able to object to the *profiling* of their data based on a public interest or a legitimate interest.

15.2. The Company shall cease *processing* unless it has compelling legitimate grounds to continue to process the *personal data* which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

15.3. The individual has the right to object to their *personal data* for direct marketing.

16. Enforcement of Rights

16.1. All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

16.2. The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision-making processes or profiling within one month of receipt of the request. ACG may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

16.3. Where ACG considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature, the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

17. Automated Decision Making

17.1. ACG will not subject individuals to decisions based on automated *processing* that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the *data controller* and the individual;
- Is authorised by law; or
- The individual has given their explicit *consent*.

18. Data Breaches

Reporting Personal data breaches

18.1. All data breaches should be referred to the persons whose details are listed in the Appendix.

***Personal data breaches* where ACG is the *data controller*:**

18.2. Where ACG establishes that a *personal data breach* has taken place, the company will take steps to contain and recover the breach. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

18.3. Where the *personal data breach* happens outside the UK, ACG shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

***Personal data breaches* where the Company is the *data processor*:**

18.4. The Company will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

Communicating *personal data breaches* to individuals

18.5. Where ACG has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

18.6. ACG will not be required to tell individuals about the *personal data breach* where:

- The company has implemented appropriate technical and organisational protection measures to the *personal data* affected by the breach, in particular to make the *personal data* unintelligible to any person who is not authorised to access it, such as encryption.
- The company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, the company shall make a public communication or similar measure to tell all affected individuals.

18.7. All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life (Article 8)
- Freedom of thought, belief and religion (Article 9)
- Freedom of expression (Article 10)
- Freedom of assembly and association (Article 11)
- Protection from discrimination in respect of rights and freedoms (Article 14)

If you have a complaint or suggestion about the Company's handling of *personal data* then please contact the person whose details are listed below:

Data Queries or Subject Access Requests including removal/Restrictions of data

E-mail IGT@activecaregroup.co.uk or write to

Data Protection Officer

Active Care Group Support Centre

1 Suffolk Way

Sevenoaks

Kent

TN13 1YL

Alternatively, you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

19. Training Requirements

19.1. All staff shall be inducted into the business with a plan that includes Information Governance, Data Protection and Confidentiality. It is the responsibility of Heads of Department and Line Managers to ensure that all staff are aware of and understand the importance of only processing data that they are lawfully permitted to process and in accordance with this policy.

20. Policy Review Statement

20.1. This document may be reviewed at any time at the request of either staff or management, but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

21. Associated Documents

- Information Governance Policies

- Data Protection Policies
- Privacy Policies and notices
- Subject Access Request Policy

22. Associated References and Further Guidance

- Data Protection Act 2018
- General Data Protection Regulations (GDPR) 2018
- Human Right Act 1998
- The Care Act 2014

23. Audit and Monitoring

Objective	Lead	Measure	Frequency	Reporting
To ensure compliance with Data processing	Data Protection Lead	Reporting Breaches via the Breach Register	Monthly	Quality and Governance Report

24. Document Change History

Version	Description of revision (include reason for revision)
1	Initial Version
2	Page 13 email address change to Active Care Group. Data Protection Lead changed to Data Protection Officer.