Privacy and Personal Data Protection and Retention Policy

Document Classification:	**Confidential**
Draft	**April 2018**
Last Revised /Reviewed	**September 2019**
Review Due	**September 2021**
Document Owner:	**DPO**

Action for Carers (Surrey) is a company Limited by Guarantee with Charitable status. Charity No. 1116714.
Registered office: Astolat, Coniers Way, Burpham, Guildford, GU4 7HL Company No: 5939327

Contents

List of Tables

1 Introduction

In its everyday business operations, Action for Carers Surrey makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Carers/Clients
- Users of its websites
- Supporters
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Action for Carers Surrey is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Action for Carers Surrey systems.

The following policies and procedures are relevant to this document:

- *Data Protection Procedures for staff and volunteers*
- *Data Subject Request Procedure*
- *Information Security Incident Response*
- *Data Breach Notification procedure*
- *IT and Communications Procedures for staff and volunteers*
- *Codes of Conduct working with Children and Young People*
- *Data Protection Impact Assessment*
- *Confidentiality Policy*
- *Information Classification Procedure*

3 Privacy and Personal Data Protection Policy

3.1 The General Data Protection Regulation and Data Protection Act 2018

The General Data Protection Regulation 2016/679 (GDPR) is one of the most significant pieces of legislation affecting the way that Action for Carers Surrey carries out its information processing activities. Significant fines may be applicable if a breach is deemed to have occurred under the GDPR. It is Action for Carers Surrey's policy to ensure that our compliance with the GDPR, the Data Protection Action 2018 and other relevant legislation protecting the personal data of citizens of the UK is clear and demonstrable at all times.

3.2 Definitions

There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means*:*

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' means*:*

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

3.3 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which data protection legislation is based.

These are as follows:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, 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 ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) 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 ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Action for Carers Surrey must ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

3.4 Rights of the Individual

The data subject also has rights under data protection legislation. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within Action for Carers Surrey that allow the required action to be taken within the timescales stated in current data protection legislation.

These timescales are shown in Table 1.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) Within a reasonable period after obtaining the personal data, but at the latest within one month (if not supplied by data subject)
The right of access	Without undue delay and in any event within one month of receipt of the request
The right to rectification	Without undue delay and in any event within one month of receipt of the request
The right to erasure	Without undue delay and in any event within one month of receipt of the request
The right to restrict processing	Without undue delay and in any event within one month of receipt of the request
The right to data portability	Without undue delay and in any event within one month of receipt of the request
The right to object	Without undue delay and in any event within one month of receipt of the request
Rights in relation to automated decision making and profiling.	Without undue delay and in any event within one month of receipt of the request

Table 1 - Timescales for data subject requests

The timescales for responding to each of the rights set out above (with the exception of the right to be informed) may be extended by a further two months where necessary, taking into account the complexity and number of the requests. In such cases, Action

for Carers Surrey must inform the data subject of the extension within one month of receiving their request and must give the reasons for the delay.

3.5 Consent

Unless Action for Carers has an alternative basis under current data protection legislation for using personal data, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 parental consent must be obtained. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

3.6 Privacy by Design

Action for Carers Surrey has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation should be considered where applicable and appropriate.

3.7 Transfer of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

If there is no adequacy decision in place, Action for Carers Surrey will usually enter into the European Commission's Standard Contractual Clauses with the third party located outside the European Union.

3.8 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, Action for Carers Surrey has appointed the following Data Protection Officers:
Jamie Gault
Anne Hess

3.9 Breach Notification

It is Action for Carers Surrey's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. In the UK, the DPA is the Information Commissioner's Office (the "ICO"). This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

Under current Data Protection Legislation the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the GDPR.

3.10 Addressing Compliance to Data Protection Legislation

The following actions are undertaken to ensure that Action for Carers Surrey complies at all times with the accountability principle of the GDPR and the Data Protection Act 2018:

- The legal basis for processing personal data is clear and unambiguous
- A DPO is appointed with specific responsibility for data protection in the organization
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes

- The following documentation of processing activities is recorded:
    - Organization name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the general information security management system.

4.0 Records Retention and Protection Policy

Introduction

In its everyday business operations Action for Carers Surrey collects and stores records of many types and in a variety of different formats. The relative importance and sensitivity of these records also varies and is subject to the organization's security classification scheme.

It is important that these records are protected from loss, destruction, falsification, unauthorised access and unauthorised release and range of controls are used to ensure this, including backups, access control and encryption.

Action for Carers Surrey also has a responsibility to ensure that it complies with all relevant legal, regulatory and contractual requirements in the collection, storage, retrieval and destruction of records. Of particular relevance, is the Data Protection Act 2018, the GDPR, and guidance published by the ICO and/or the European Data Protection Board concerning the storage and processing of personal data.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Action for Carers Surrey systems.

This section begins by establishing the main principles that must be adopted when considering record retention and protection. It then sets out the types of records held by Action for Carers Surrey and their general requirements, before discussing record protection, destruction and management.

4.1 General Principles

There are a number of key general principles that should be adopted when considering record retention and protection policy. These are:

- Records should be held in compliance with all applicable legal, regulatory and contractual requirements
- Records should not be held for any longer than required
- The protection of records in terms of their confidentiality, integrity and availability should be in accordance with their security classification
- Records should remain retrievable in line with business requirements at all times

4.2 Record Types and Guidelines

In order to assist with the definition of guidelines for record retention and protection, records held by Action for Carers Surrey are grouped into the categories listed in the table below. For each of these categories, the required or recommended retention period are given, together with a reason for the recommendation or requirement.

Note that these are guidelines only and there may be specific circumstances where records need to be kept for a longer or shorter period of time. This should be decided on a case by case basis as part of the design of the information security elements of new or significantly changed processes and services.

Further information about records held by the organization, including their security classifications and owners can be found in *Information Asset Inventory*.

4.3 Key Data Retention Periods:

Category	Description	Retention period	Reason
Accounting	Annual Accounts, Management Accounts, Payroll, Pensions, Invoices, Bank Statements, Grants and Contracts	6 years from the end of the financial year in which the transaction was made	Statutory
Governance	Incorporation Record, Articles of Association, Resolutions, Minutes of Board Meetings and Sub Groups, Register of Directors, Register of Members	Permanently	Statutory
Contractual	Legal contracts, terms and conditions, leases	6 years after contract end	Maximum period within which dispute might occur
Insurance Records	Public Liability, Employers Liability	Permanently/40 years	Employers' Liability (Compulsory Insurance) Regulations 1998
Accident Records	Accident Record Books	3 years from date of entry	Health and Safety at Work Act 1974 S7
Client Records Adults	Client data and case notes	7 years from the date Action for Carers Surrey ceases providing services to the Client	Statutory limitation period for claims
Client Records Children	Client data and case notes * Note a record becomes archived information for a non-participating young person at 18th birthday. For participating young person at 25th birthday	6 years from the date it becomes archived (*18th or 25th birthday)	In Line with SCC Children's Services retention period for accessible child records.
Client Records	Records of initial contact – Client decides not to use our services	6 months	Statutory, with reference to limitation period for bringing a claim under the

			Equality Act 2010
Human resources	MOT Certificate, Insurance certificate, Driving Licence, paperwork relating to DBS check, Emergency contacts Information	6 months from termination date	Statutory
	Recruitment records for unsuccessful applicants	6 months	Statutory, with reference to limitation period for bringing a claim under the Equality Act 2010
	Right to work in the UK evidence	2 years	Statutory
	Personnel File – Contract of Employment, Correspondence, Recruitment documentation, and documentation relating to leaving employment.	6 years from termination date	Statutory
	Statutory Maternity Pay records, calculations, certificates or other medical evidence	Three years after the end of the tax year in which maternity period ends	The Statutory Maternity Pay Regulations
	Statutory Sick Pay records, calculations, certificates, self-certificates	Three years after the end of each tax year for Statutory Sick Pay purposes	Statutory Sick Pay (General) Regulations
	Pension records re: current pensioners	10 years after benefit ceases	Commercial