Data Protection Policy v1.0

AdvoCard

Last updated	December 2018

1. **Introduction**

AdvoCard is an independent advocacy service for mental health service users in Edinburgh. AdvoCard processes personal data and special category personal data in relation to the users of its services and the individuals that deliver the services. As a Data Controller, AdvoCard is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR).

2. **Scope**

This policy applies to the processing of all personal data used to deliver an independent advocacy service and related activities by AdvoCard is respect of service users, employees and volunteers. All employees and volunteers who deliver AdvoCard's services, including its partner agencies (Edinburgh Carers Council and the Royal Edinburgh Hospital Patients Council), must comply with this policy.

3. **Definition of Personal Data**

Personal data is information relating to a living individual or an identifiable living person (known as a Data Subject). An identifiable natural person is one who can be identified directly or indirectly by reference to an identifier such as a name, ID number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

4. **Data protection principles**

The data protection principles are obligations that must be followed, the details of which are set out below.

4.1 *Personal data should be processed lawfully, fairly and in a transparent manner*

This means that personal data must not be processed

- without having a lawful basis (e.g. legitimate interests or consent)
- in a way that the individual wouldn't reasonably expect
- in a way that is transparent to the individual

4.2 *Personal data should be collected for specified, explicit and legitimate purposes*

This means that personal data must only be used for the reason that it was obtained from the individual.

4.3 *Personal data should be adequate, relevant and limited to what is necessary*

That means that AdvoCard must only obtain the personal data needed to achieve the purpose.

4.4 *Personal data should be accurate and where necessary kept up-to-date*

This means we must take all reasonable steps to ensure that personal data is accurate and kept up-to-date; inaccuracies should be promptly corrected.

4.5 *Personal data should be kept for no longer than is necessary*

This means that personal data must not be kept longer than is needed to achieve its purpose. Personal data must be disposed of in accordance with the retention schedule set out in the Record of Processing.

4.6 *Personal data should be processed in a manner that ensures appropriate security*

This means that we must have appropriate technical and organisational measures in place that ensures the security of personal data to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.7 *Accountability Principle*

This means that AdvoCard must demonstrate compliance with the data protection principles and provide evidence of compliance with the principles.

5. General Obligations

The GDPR introduced other specific obligations and these are set out below.

5.1 Data Protection by Design and Default

When designing new systems or modifying existing systems we must consider the privacy needs of individuals and build in privacy and security requirements from the beginning.

5.2 Record of Processing

A Record of Processing that sets out AdvoCard's processing activities is in place and must be kept up-to-date.

5.3 Security of Processing

AdvoCard must ensure a level of security appropriate to the risk associated with the processing. This means:

- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- having the ability to restore the availability and access to personal data in a timely manner in the event of an incident
- applying access controls to personal data to restrict access on a "need to know" basis

- ensuring that anyone who has access to personal data does not process that information unless they have authorisation

5.4 *Data Processors (e.g. suppliers)*

If AdvoCard contract with any external organisation which processes personal data on its behalf AdvoCard must only use suppliers that implement appropriate technical and organisational measures to ensure the protection of individuals' rights and a level of security appropriate to any risk associated with the processing.

5.5 *Data Breach*

Actual and suspected personal data breaches must be reported immediately to the Managing Director who will investigate the incident and inform the Board of Directors.

The Information Commissioner's Office must be notified of a "reportable" data breach within 72 hours. The Managing Director (or delegated authority) will conduct a risk assessment to determine if the data breach is likely to have an impact on the individual(s) rights and freedoms and therefore reportable to the ICO. The individual(s) may also need to be informed.

5.6 *Data Protection Impact Assessment*

A Data Protection Impact Assessment must be carried out where new technologies are being used and where there is a potential risk to the privacy and rights of individuals. The Director will be responsible for carrying this out and submitting it to the Board of Directors.

6. Individuals' Rights

The GDPR gives individuals a number of rights and AdvoCard must ensure that its systems, policies, processes and practices are designed to enable individuals to exercise their rights.

6.1 *Right to transparency*

An individual has the right to be fully informed about the collection and use of their personal data. This will be set out in a Privacy Statement that will be posted on our website. The information in the Privacy Statement must be concise, intelligible, written in clear and plain language and easily accessible.

6.2 *Right to access personal data held about them*

An individual has the right to request access to the personal data we hold about them; this is known as a Data Subject Access Request and it can be submitted in writing or verbally. We must respond to a subject access request within one month. There is no charge for this service.

Personal data must be provided if held and must not be modified before being provided to the individual.

6.3 *Right to rectification*

An individual has the right to request that any inaccurate personal data we hold about them is corrected.

The following rights only apply in specific circumstances so we may not be obliged to agree to a request.

6.4 *Right to erasure*

An individual has the right to request erasure of their personal data.

6.5 *Right to restriction of processing*

An individual has the right to request restriction of processing of their personal data.

6.6 *Right to data portability*

An individual has the right to receive the personal data held about them in a structured, commonly used and machine-readable format and have the right to transmit the data to another organisation.

6.7 *Right to object*

An individual has the right to object to the processing of personal data and have it stopped in specific circumstances.

6.8 *Right not to be subject to automated decision-making or profiling*

An individual has the right not to be subject to automated decision making and/or profiling. These are decisions or evaluations of certain things about an individual made solely by automated means.

7. Data Sharing

We may be asked to consider putting in place a data sharing arrangement in some circumstances. If that happens

- No sharing can happen until a formal and signed data sharing arrangement is in place
- The individual whose data is being shared must be informed and where necessary consent should be obtained

8. Responsibilities

8.1 Board of Directors

The Board of Directors is responsible for:

- Approving this policy
- Approving data protection impact assessments (where needed)
- Overseeing the handling of a data breach

8.2 Managing Director of AdvoCard

The Managing Director of AdvoCard (or delegated authority) is responsible for:

- Updating this policy at least annually
- Ensuring that appropriate arrangements are in place to comply with GDPR
- Ensuring that all employees and volunteers are aware of and understand the requirements of this policy
- Preparing data protection impact assessments (where needed)
- Managing an actual or suspected data breach or breach of privacy
- Managing any rights request exercised by a data subject (e.g. data subject access request)
- Ensuring that formal data sharing requests are put in place where needed
- Ensuring that adequate access controls are in place and reviewed at least annually

8.3 Employees and Volunteers

Employees and volunteers are responsible for:

- Complying with this policy
- Reporting any actual or suspected data breach or breach of privacy to the Director of AdvoCard as soon as they become aware
- Completing any training as required by AdvoCard

9. Compliance

A deliberate disclosure of personal data, non-compliance with the data protection principles or breach of an individual's privacy may constitute gross misconduct and lead to termination of contract.

10. Glossary

Special category personal data means personal data that relates to:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership status
- physical or mental health or condition
- sexual life

Processing includes creating, obtaining, recording, storing or using the personal data – anything from getting it, moving it, analysing it, reading it, sharing it with anyone, storing it, deleting or destroying it.

Data controller refers to an organisation or individual who decides the purpose and manner in which personal data should be processed.

Data processor is an organisation or an individual who processes personal data on behalf of a data controller, eg printer, courier, software development contractor.

Data subjects are living people about whom the personal data is held.

Data subject access request is a request from a data subject, or an authorised third party, for access to personal data about them that is held by the organisation

Reportable data breach is one that affects the rights and freedoms of individuals.

Technical security measures are measures to protect information held on systems, such as network security, malware prevention, encryption and back-ups.

Organisational security measures support technical measures, and include policies and procedures, training and awareness, and access controls.

Confidentiality means to provide access to information for only those individuals with a valid and authorised reason to do so

Integrity means ensuring that information is not altered/deleted or tampered with. Information must be accurate, up-to-date and trusted

Availability means ensuring that information is available to authorised individuals who need it, when they need it