



Data Protection Policy

Background

The Data Protection Act came into force in 1998 and regulated the processing of information relating to living and identifiable individuals (data subjects). This included the obtaining, holding, storing, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

General Data Protection Regulations (GDPR) replaces the current Data Protection Act. These new regulations come into force in May 2018. The regulations will be adopted as law by the UK Government at the time of Brexit.

The legislation places obligations on organisations to protect the rights of people whose personal information they hold – this could be employees, volunteers and those accessing services.

We will ensure that data users comply with the data protection principles of good practice which underpin the new regulations.

Personal data must be:

- Obtained and processed fairly and lawfully
- Held only for specified purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with the regulations
- Kept secure and protected at all times

It is the policy of ECC to ensure that all personal data will be held in accordance with the principles and requirements of GDPR data protection and procedures will be put in place to ensure the fair processing of data subjects.

We will also adopt a clear **Retention Policy** and **Breach policy** to ensure that everyone dealing with data is aware of their individual and collective obligations.

We expect all ECC employees who process, or use personal data will ensure that they abide by these principles at all times.

ECC is the data controller under the Act and is therefore ultimately responsible for implementation.

It is the responsibility of the Data Protection Officer (Coordinator) to oversee day to day matters, notification, and contact with the ICO (Information Commissioners Office) ensuring that this data protection policy and compliance is reviewed at appropriate levels, intervals and the handling of subject access requests.

Relevant data protection issues / direction will be included in all employee and volunteer induction.

Purposes of Collecting and Recording Personal Information

The main purpose for keeping agency records on people who access our services is to enable us to deliver services. Information about individuals will only be collected and recorded with good reason. It will be stored securely and only for as long as required.

We gather these details in a number of ways however we will always ask for express permission to hold this information

We collect names, addresses and contact details as well as any particular adjustments needed to access or use the service. This may include health information. We collect date of birth, residence and health information of the person cared for

Information about individuals will not be published in any type of directory without the written consent of the individual.

No details of individuals will be passed to other organisations for marketing, fundraising or circulating information.

The website will contain a link to our **Privacy Policy / Statement**

Photographs, recordings, videos or DVDs in which individuals are identifiable will only be used with their explicit written consent.

Manual files containing sensitive information about individuals will be labelled confidential and kept in locked filing cabinets, accessible only to relevant employees.

Computer files containing sensitive information about individuals will be password protected.

HR records

Personnel records, including employment, salary records, supervision and appraisals, are held in strictest confidence for effective management of resources and to comply with employment and company legislation.

We will work proactively with Advocard to ensure that these meet the requirements of GDPR

We are required to take up relevant reference checks for the recruitment of both employees and volunteers, particularly to safeguard the health and safety of employees, volunteers and those using our services. Please refer to Advocard Recruitment protocols for further information.

We are also required to take up an enhanced disclosure and PVG checks for all relevant volunteers and employees. Please refer to our Disclosure Policy for further information.

All of the information and data we request and collect from people using our services is treated with the strictest confidence.

Relevant data protection issues will be included in all induction and training

An internal audit of data protection compliance will be carried out at appropriate intervals (Suggest 6 monthly)

Transfer of information

In any situation where a person's safety is considered to be at risk then further action may be necessary and other agencies contacted. In these circumstances we will comply with statutory requirements relating to protection of vulnerable groups, or health and safety at work.

Retaining information –

We will not keep information on individuals for longer than is necessary, but we need to retain some information for several years to meet our duties as an employer, a company and a service provider. Article 5 (e) of the GDPR states that personal information should be kept for no longer than is necessary for the purposes for which it is being processed

Edinburgh Carers Council will:

- Check with carers annually whether they wish personal information to be kept or updated for mailing purposes.e.g Newsletters and Events
- Delete and destroy advocacy casenotes (individual and groups) after 6 years (NB Advocard practice)
- Ensure that personal information is securely disposed of when no longer needed e.g. destroying paper copies in confidential waste and deleting emails and online records
- Achieve good practice in employee data retention e.g. HR records in summary file retained for 6 years after the employee has left the organisation before all information is destroyed. Recruitment information kept securely for 1 year before being destroyed (link to full retention policy)

Access to Records - Your right to information

Under the terms of the GDPR you have the right to request a copy of any personal data you believe may be held about you. You are also entitled to have any information corrected if it is wrong.

If you request to see your file you should write to us to request this. You will receive access to personal data held by us within 40 days.

If you request and see your personal data we will only supply information from the date of the last request.

There are certain circumstances where it is not possible for us to comply with a request for information, for example where we could not provide information to the subject without revealing information about another person or third party.

In these situations, we will take advice from the Information Commissioner's Office to ensure that we comply with GDPR in terms of the rights of each person involved.