



DATA PROTECTION AND CONFIDENTIALITY POLICY

Introduction

SNAPS has a duty of care with regards to the Data Protection and Confidentiality of information stored in relation to the families using our services. SNAPS regards the lawful and correct treatment of personal data as an integral part of its function and vital for maintaining confidence between families and ourselves. This policy applies to all employees, contractors, volunteers, Trustees and families who come into contact with personal information.

For the purposes of this policy data refers to information which:

- Is being processed by means of equipment operating automatically in response to instructions given for that purpose,
- Is recorded with the intention that it should be processed by means of such equipment,
- Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
- Forms part of accessible records,
- Includes disclosure under the Disclosure and Barring Service,
- Is not kept for longer than necessary.

Aim

The aim of this policy is to provide the employees, contractors, volunteers, Trustees and families using SNAPS' services with a framework for the lawful, secure and confidential processing of personal data in accordance with the Data Protection Act 2018 (which has been incorporated into UK data protection law in January 2021 after the UK's withdrawal from the EU). SNAPS has up-to-date registration under the Data Protection Act with the Information Commissioner's Office.

SNAPS will through appropriate management and controls:

- Observe fully the conditions regarding the fair collection and use of information,
- Meet its legal obligation to specify the purposes for which its information is used,
- Collect and process appropriate information and only to the extent that it is need to fulfil operational needs or to comply with any legal requirements,



SNAPS YORKSHIRE CIO DATA PROTECTION AND CONFIDENTIALITY POLICY MAY 2025

- Ensure the rights of people for about whom information is held can be fully exercised under the act,
- Take appropriate technical or organisational security measures to safeguard personal data,
- Ensure that personal data are not transferred without suitable safeguards.

Roles and responsibilities

SNAPS will ensure that everyone managing and processing personal data understands that they are contractually responsible for following good data protection practice and where appropriate are bound by common law duty of confidence. These responsibilities apply to all persons who have contact with SNAPS.

SNAPS' Chief Executive is the appointed Data Protection Officer. The officer will ensure that legislation requirements are met as well as ensure that all employees adhere to legislative requirements.

SNAPS will specifically ensure that everyone managing and handling personal data is appropriately trained to do so.

Methods of handling personal data are clearly described.

In response to the new GDPR legislation in 2018, SNAPS updated its data handling procedures and policies. GDPR's seven principles are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability. Only one of these principles – accountability – is new to data protection rules. In the UK all the other principles are similar to those that existed under the 1998 Data Protection Act as outlined above.

For SNAPS, accountability means documenting how personal data is handled and the steps taken to ensure only people who need to access some information can. It also means training employees in data protection measures and regularly evaluating and data handling processes.

The "destruction, loss, alteration, unauthorised disclosure of, or access to" people's data where it could have a detrimental impact on those who it is about, must be reported to the ICO, the UK's data protection regulator. SNAPS' Data Protection Officer will ensure that if a breach occurs, the ICO will be informed within 72 hours after an organisation finds out about it. SNAPS would also tell the people the breach impacts.



SNAPS YORKSHIRE CIO DATA PROTECTION AND CONFIDENTIALITY POLICY MAY 2025

All employees complete a GPDR declaration when they join the organisation to be transparent in how we hold and use their data. All of SNAPS' electronic mailings have an option to be removed from our mailing lists.

SNAPS will ensure that adequate training is provided for all employees involved with the processing of personal data and that qualified expertise is available for consultation.

An annual audit review will be carried out in respect of the way personal data is managed and any changes to the management of the data will be reviewed and updated accordingly.

Amendments will be made to the policy where necessary and all employees will be informed and training given where appropriate.

<p>Drafted: 05/05/2025 Approved By Board: 14/05/2025 Next Review Date: 05/2026</p>
--