North Yorkshire Advocacy

Enabling people to speak up for themselves

Case Recording and File Storage

North Yorkshire Advocacy will keep detailed records of all client contact in line with the Data protection Act 1998 and General Data Protection Regulation 2018

1. Data Storage

1.1 All paper files will be stored in secure locked filing cabinets within North Yorkshire Advocacy offices.

1.2 All client contact will be recorded on the data management system Blue Door where possible through scanning and direct input. Any additional papers to be stored as 1.1 if absolutely essential to client support needs or else destroyed.

1.3 Each member of staff with authorised access to client record management system will maintain a personal password to the system.

1.4 North Yorkshire Advocacy employees and volunteers will not record personal opinion, or the personal opinion of others, in files. All information should be factual and objective.

1.5 North Yorkshire Advocacy employees and volunteers will keep a record of all work undertaken on behalf of a client and all case files will be destroyed after 4 months of closure. Information in files that are active may contain only contain information which is relevant to the current support needs of the client. Clients may have information returned to them if that is their wish. Information recorded will include engagement and time taken, and completion will be recorded.

2. Data Sharing

2.1 Any confidential information which is to be sent by email must be sent in a password protected word document or anonymized using the client reference number

2.2 Files will not be accessible to other individuals or agencies without client consent and permission.

2.3 Anonymised and Statistical information will be recorded and made available to regulatory bodies.

2.4 North Yorkshire Advocacy will keep comprehensive records of referrals. The information kept will support a quantitative and qualitative analysis. North Yorkshire Advocacy will operate a policy that accommodates the information and acknowledges that in certain circumstances it may need to be disclosed to the courts.

3. Data Access

3.1 All data whether personal or organisational must be secured by a password

3.2 All data sent electronically must be password protected

3.3 All passwords must be changed on a quarterly basis.

3.4 No employees or volunteers of North Yorkshire Advocacy must share or use another's password.

3.5 Working remotely, Employees and Volunteers must ensure that all computer equipment is virus protected with regularly updated reputable software. All data must be saved to a mobile device and kept in a locked unit.

3.6 No paper files or computer equipment belonging to or containing North Yorkshire Advocacy information or data must be left unattended outside of office premises.

3.7 Releasing data to the public, including family and friends will be considered an act of gross misconduct and will result in dismissal.

Data Protection Act 1988 – Eight Core Principles:

1 Personal data must be processed fairly and lawfully.
2 Personal data must be obtained only for one or more specified and lawful purpose and must not be processed in a manner incompatible with that purpose.
3 Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4 Personal data must be accurate and where necessary, kept up to date.
5 Personal data processed for any purpose must not be kept for longer than is necessary for that purpose.
6 Personal data must be processed in accordance with the data subject's rights under the Act.
7 Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage, to personal data.
8 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to processing personal data.