Country Days

Data Protection Policy

Approved by:	Rita Di Carlo Head of Administration	Rita Di Carlo
Last reviewed on:	March 2025	
Next review due by:	March 2026	
Date:	March 2025	

The following policy sets out the framework for the collection, processing and security of data needed to deliver our services, which is designed to achieve a high level of protection for Country Days - "Country Days" and its service users.

It is necessary for Country Days to hold personal data about its Personnel, Service Users, Service User families/guardians and Providers to enable the organisation to respond to and meet service needs. It is vital that Personnel who collect and use personal data comply with the requirements of the Data Protection Act 2018 and the UK GDPR.

Personnel who collect personal information must inform the individual of the purpose for which the data is being collected, which is detailed in our Privacy Notice. Once collected, this data must not be disclosed to a third party without a lawful basis, except where legally obliged to do so.

Country Days is fully committed to compliance with the Data Protection Act 2018 and with the requirements of the UK GDPR, (henceforth referred to as "the Acts") and abides by their provisions. Country Days will therefore follow procedures that aim to ensure that all Personnel (Employees, Trustees, contractors, volunteers) have access to any personal data held by or on behalf of the company, are fully aware of and abide by their duties and responsibilities under the Acts.

Informing Service users about Confidentiality Standards

Service users are informed that any information held is treated as confidential, stored in a secure manner and accessed only by Country Days staff, volunteers and agreed partners. Service users are to be informed how the information gathered may be used and what their rights are in respect of their data via Country Days's Privacy Notice.

There are certain exceptions to the above such as in cases where there is clear evidence of serious risk to an individual or to the welfare of others. No guarantee of confidentiality will be given in the following circumstances:

• Where child protection/vulnerable adult issues are involved

• Where there is significant threat to life

• Where a Service user needs urgent medical attention

• Where information regarding a criminal offence is disclosed

• Where a breach of a statutory provision is concerned

Service user Permission to Disclose Information

A service user has the right to expect that information given in confidence will be used only for the purpose for which it was given and that it will not be disclosed to others without permission unless there is an overriding obligation or duty to pass on that information. Explicit permission should always be sought and appropriately logged when the service user subscribes for the service. If a service user has a language difficulty the implications of obtaining the consent will be clearly explained. If required a translation service will be used. It must be emphasised to service users that only relevant information will be passed on. Country Days Personnel will ensure that Service users understand that the information is available to Country Days Personnel for the purposes of providing our services to them.

Confidentiality and Recorded Information

Information collected and recorded should:

• reflect the needs of the service user

• be as up to date and accurate as possible

• be factual information about what was discussed along with any relevant implications and is as free as possible from any bias

• should be non-judgemental

• avoid stating opinions unless evidence exists to support it

• be relevant

• be recorded concisely and legibly, using appropriate language

• be initialed and dated either physically or digitally

• be, where possible, agreed with the service user.

In recording information gained from third parties it is made clear from whom the information has been obtained.

Storage of Records and Access

Information relating to service users is held confidentially and is stored securely on a secure IT system.

Personnel must ensure when information is in use that it is not accessible to third parties by:

• not leaving written information unsecured where it could be read by others

• ensuring that information on electronic devices is not visible to others and such devices are ‘screen locked’ when not in use or unattended

• ensuring individually identifiable information held on computer is protected from inappropriate access by use of access passwords

• not discussing information relating to a Service User within the hearing of others who should not have access to this information

• Access to Service User's records is restricted to Country Days staff (and, where appropriate, agreed partners & volunteers) in order to carry out their duties.

Personnel will only access individual Service User records when they have a legitimate purpose for doing so. Examples of legitimate purposes are in order to provide services to service users, or for staff development in relation to use of the system.

A Service User, current or former, asking to see their file or items contained within it should be referred to the Data Protection Officer (info@countrydays.net) and the request will be handled as a Subject Access Request in line with the Acts.

Implementation

The Data Protection Officer (contactable on info@countrydays.net) has responsibility for:

• Undertaking risk assessments and taking steps to ensure that risks are mitigated, reporting to the Trustees as necessary

• The provision of data protection training, for staff in conjunction with the HR function

• The development of practice guidelines and procedures

• Carrying out compliance checks to ensure adherence to the Acts and this policy

• Developing information sharing protocols between the component member organisations within Country Days

• Any necessary recording and reporting of incidents breaching the Acts and/or this policy to the ICO