Triratna Safeguarding and Data Protection 2026

UK Triratna charities and the Equality Act 2010 and UK General Data Protection Regulation 2018

This is a guidance document for you to refer to, not a policy to be adopted. Based on law and best practice in the UK, it should be read together with the documents listed at the end.

The trustees of UK charities are responsible for ensuring that their employees and volunteers observe legislation in regard to equalities and data protection.

Equalities legislation

The Equality Act 2010 prohibits discrimination in the provision of goods and services against people with nine “protected characteristics”:

- age
- race
- religion or belief
- sex
- sexual orientation
- disability (including mental health disability)
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity

1. This means a Triratna charity may not prevent from using its services someone who holds a protected characteristic, unless it can prove that to do so is ‘objectively justified’.
2. So, for example, a Triratna charity must not treat a person with mental illness unfavourably because of anything connected with their condition, unless the charity can show that it is ‘objectively justified’. (This only applies if the individual or organisation knows, or could reasonably have been expected to know, that the person is mentally ill.)
3. So, when can this be objectively justified?

    - If the charity can demonstrate that it is ‘a proportionate means of achieving a legitimate aim’.
    - If challenged in court, your charity can justify its actions, providing evidence. Generalisations will not be sufficient to provide justification. It is not necessary for that justification to have been fully set out at the time the provision, criterion or practice was applied.
      Examples of legitimate aims include:

- Ensuring the health and safety of those using your services, provided risks are clearly specified;
- Ensuring the wellbeing or dignity of *everyone* using your services; for example, everyone on a retreat.

So, your charity may decline to provide retreats, meditation courses etc to individuals with protected characteristics where you can reasonably demonstrate that you are unable to ensure the health and safety of those taking part (e.g. where an individual's factually described mental health problems or level of physical disability mean that you cannot ensure their health and safety or that of others, or the wellbeing or dignity of others on the course or retreat.

Data protection and Safeguarding

The UK General Data Protection Regulation operates alongside an amended version of the Data Protection Act 2018.

The law permits the sharing of personal data for certain purposes to do with criminal justice and Safeguarding. In particular, the Act permits the sharing of information for

- the prevention or detection of crime; and
- the capture or prosecution of offenders
- specifically for the Safeguarding of children and adults who may be at risk.

This means you may share with police or social services or another charity's Safeguarding Lead information/concerns about a particular individual who may pose a risk to themselves or to others. For example, if a sex offender attends your centre and you know they are also visiting another centre or retreat centre, you should share information with the retreat centre's Safeguarding Lead, Safeguarding trustee or Chair.

Your Safeguarding Lead should record in your charity's Safeguarding log your reasons, clearly and objectively, being prepared to account for your decisions and actions if required.

This means you must

- **Be factual.** (Describe the mental health diagnosis/disability/etc and the particular symptoms which make the provision of the service unfeasible on the grounds outlined above.)
- **Describe** the 'objective justification' for **each** case.
- **Set a time limit**. (You cannot bar people indefinitely but must review at regular intervals.)
- **Clarify whether there are any adjustments which could be made** to enable access to services. (eg, would bringing a mental health carer with them make it possible for an individual to attend a retreat?)

Summary

1. When keeping records of personal/sensitive information about a person you must record your observations and thinking in a style you would be happy to share publicly if requested; ie objectively, factually and respectfully, demonstrating care for the wellbeing of all concerned.
2. You may not hold or share informally internal written information about anyone who uses your centre or retreat centre; for example a little book of notes for team use only.
3. You may share formally written personal information very selectively where there are justifiable legal or Safeguarding concerns.
4. You must explain to users that you hold and share personal data/ sensitive information about them
5. You must explain what constitutes “personal data/sensitive information”.
6. You must explain where and how you hold the information and the circumstances under which you use it and share it.
7. You must explain that the subject can make a ‘Subject Access Request’ to access any sensitive information you hold about them.

More general data protection advice for small- and medium-sized charities and ‘third sector ‘organisations

1. **Tell people what you are doing with their data.**
People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

2. **Make sure your teams, teachers and volunteers are adequately trained**.
When you take on new people to help run your Buddhist centre/retreat centre, they need to receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.
3. **Do not keep people’s personal information on computers.**
Personal information (eg Safeguarding logs) should be stored on password protected cloud drives such as Google Drive or Proton Drive. This is to protect it from being accessed should a computer be hacked.
4. **Encrypt/lock away external drives/memory sticks**
All portable devices – such as memory sticks and laptops – used to store personal information should be encrypted or locked up and accessible only to those authorised to access them because they have a ‘reasonable need to know’ in order to carry out their roles within your charity.
5. **Storage of records -** We should now NOT be storing paper copies or data on memory sticks but using secure online storage. I am using Proton Drive for archived information and Google Drive for current cases and email logs. I upload them to proton drive after a few months of the case finishing/monthly log finishing. PLEASE DON’T USE PERSONAL GMAIL GOOGLE DRIVES! We have a charity specific one that can be passed on to a new Safeguarding Lead when you leave.

You can get free help from

- the Information Commissioner's Office https://ico.org.uk/for-organisations/
- external Safeguarding experts such as Thirtyone:eight www.thirtyoneeight.org

This document is to be read in conjunction with:

Model Child Protection Code of Conduct 2026

Model Child Protection Policy 2026

Model Adult Safeguarding Policy 2026

Model Ethical Guidelines 2026

Caring for Teenagers in Triratna 2026

Managing those who Pose a Risk 2026

Online Safety in Triratna 2026

This guidance published 2024 by Triratna's ECA Safeguarding Consultant