

Beyond Limits provides policies and procedures to promote safe and consistent practice across the Organisation. The framework laid down within our policies and procedures lets everyone know how we work and reflects our values and mission statement. Our policies and procedures are written to help us, employees of Beyond Limits, to make good, safe decisions.

Beyond Limits expects all employees to be familiar with the contents of all policies and procedures relevant to their role and to understand how to apply them within their daily work.

None of these documents stand alone, all fit within the larger framework of how we work and any associated policies which are particularly relevant will be directly referenced.

Confidentiality Policy

This policy should be read in conjunction with the Computers, IT and Social Networking Policy, Code of Conduct and Whistleblowing policy.

Confidentiality Policy – what this means to Beyond Limits:

- To support someone well, employees are required to know a lot about a person and will generate lots of information of a sensitive and private nature about the person and about Beyond Limits. Employees are required to keep this information confidential, both during their employment and after leaving Beyond Limits.
- The only exception to this is if required to disclose information by law or in the course of performing their duties with the organisation.
- Employees and Beyond Limits have legal responsibilities to keep personal data confidential and secure under the:

Data Protection Act 2018

- The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) Everyone responsible for using personal data has to follow strict rules called "data protection principles". As an organisation which processes personal data for its employees and people we support, we have a duty to ensure the information is used fairly, lawfully and transparently. Any information collected must only be used for specified and explicit purposes and used in a way that is adequate, relevant and limited to only what is necessary. As an employee, you have a responsibility to ensure that the information the

organisation holds on you is accurate and kept up to date, you must inform us of any changes to your personal information.

Human Rights Act 1998

- Article 8 states the “right to private and family life, home and correspondence.” This gives an individual the right to live their life with personal privacy in a way that does not infringe on the rights of anyone else. This could include information held on them in the form of diaries or personal records and correspondence.

Terms and conditions

- It is a requirement of your contract with Beyond Limits that you maintain confidentiality about the people we support, other colleagues and Beyond Limits. Breaking your terms and conditions could result in disciplinary action.

The Caldicott Report (1997)

- Beyond Limits supports people funded by the NHS and we therefore have a duty to appoint a guardian to ensure that we protect identifiable information that we hold about people we support. The Caldicott Guardian for Beyond Limits is the registered manager, Kathleen Scott.

Freedom of Information Act (2000)

- Information held by Beyond Limits, or information the local authority or NHS hold belonging to Beyond Limits can be requested by a member of the public for the individual of whom it relates to by completing a Freedom of Information Request. We must therefore ensure all information we keep is factual, professionally written and accurate.

Public Information Disclosure Act (1998)

- This legislation relates to our Whistle blowing policy. People who whistle blow about poor practice or corruption within Beyond Limits are protected from victimisation or dismissal.

Computer Misuse Act (1990)

- It is a criminal offence to access or destroy computer data without authority and links in with our Computer, IT and Social Networking Policy.

Beyond Limits Procedure – what we should do:

- All information kept about a person should be accurate, professionally written and factual. Information should be kept securely and only shared with people on a need to know basis.
- If you discover any personal documentation is missing for the person, this should be reported to your line manager immediately.
- How we write or talk about a person reflects how that person is perceived so think carefully about the words you use so that the people we support are always respected with the highest regard.
- You should not discuss personal information given to you by the people we support, volunteers, professionals or employees with anyone unless it is vital that the information is passed on for safety reasons. If you are unsure, please speak to your line manager.
- You should make sure your environment is private if you need to discuss confidential information.
- Any information that you give to your Service Leader or other employees of a personal nature will not be discussed with others without your consent and knowledge. The only exception to this is if there is an immediate safety issue for a person we support, an employee, or the public.
- Consult your Service Leader or the Director, immediately if you consider there may be good reason to break this rule.
- If there has been a breach in confidentiality, without good reason, you must inform your line manager immediately.
- All breaches need to be reported to the Data Liaison Officer who will follow the reporting process in the Data Protection Policy.