Data Protection & Confidentiality Policy

Primary person responsible for implementation and monitoring of this policy	Dr Kirsty Hughes kirsty@beyond-psychology.co.uk
Adopted:	May 2022
Reviewed:	January 2024
Next Review:	January 2025

Related policies and procedures: Privacy policy, Notes and record keeping policy, complaints policy and procedure.

1. POLICY STATEMENT

Everyone working for or on behalf of Beyond Psychology has a duty to keep information about patients, carers, clients, staff and other individuals confidential, and to protect the privacy of information about individuals. This duty is enshrined in law, in codes of practice issued periodically by the Department of Health, and in professional codes of conduct.

2. INTRODUCTION

This document includes guidance for staff on processing information in accordance with current legal obligations and best practice.

Beyond Psychology needs to collect and use information about people with whom it deals in order to operate. These include current, past and prospective patients, current, past and prospective employees, suppliers, clients/customers, and others with whom it communicates. In addition, it may occasionally be required by law to collect and process certain types of information to comply with the requirements of Government departments for business data.

For the purposes of this policy, the terms 'data' and 'information' are used interchangeably.

3. CONTEXT

The Data Protection Act (1998) defines a legal basis for the handling in the UK of information relating to living people. The General Data Protection Regulation, in force in the UK from 25 May 2018, updates the Data Protection Act and introduces new requirements for public authorities who handle personal data.

Beyond Psychology maintains a firm commitment to the following principles:

- Justify the purpose for collecting or holding personal data
- Do not use personal data unless it is absolutely necessary
- Use the minimum necessary personal
- Access to personal data should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share personal data can be as important as the duty to respect service user confidentiality

4. PURPOSE

The purpose of this policy is:

- To ensure any personal information collected and held by Beyond Psychology is processed fairly and lawfully
- To promote best practice in the processing of personal information
- To ensure that Beyond Psychology staff involved in processing personal information understand their responsibilities and obligations
- To ensure that Beyond Psychology staff responsible for the processing of personal information are adequately trained to fulfil their responsibilities and obligations
- To outline the procedure for reporting and investigation of a suspected breach of Confidentiality and/or Data Protection.
- To provide assurance to our patients, staff and others with whom we deal that their personal information is processed lawfully and correctly and held securely at all times.

5. SCOPE

This policy relates to all types of information within Beyond Psychology. These include:

- Client/Service User information
- Personnel information
- Organisational information.

This policy covers all aspects of information, including (but not limited to):

- Storage, filing and record systems - paper and electronic
- Transmission of information – e-mail, post, telephone and fax
- Images, including photographs

This policy applies to:

- All information systems purchased, developed and managed by, or on behalf of, Beyond Psychology
- All Beyond Psychology employees (including those on fixed term contracts) and associates

6. DUTIES

The directors have overall responsibility for Information Governance which includes the Data Protection Act 1998, including drafting policy documents, procedural guidance, training, audit and dealing with all IG related queries.

The Data Protection Officer is Dr Kirsty Hughes, who will inform and advise Beyond Psychology about its obligations to comply with the GDPR and other data protection legislation, and who will monitor compliance with those legal obligations. The DPO will manage internal data protection activities, advise on data protection impact assessments, and be the first point of contact for supervisory authorities and individuals whose data is processed.

7. DEFINITIONS

Staff: all employees and associates
Processing: Any of the following actions, in relation to the data, constitute processing:

- Obtaining
- Accessing
- Recording
- Retrieval
- Consultation
- Holding
- Disclosing
- Sharing
- Using
- Transmission
- Destruction

Data Controller: The Data Controller is the individual, company or organisation that determines the purpose and the manner in which personal data may be processed.

Data Processor: Data Processor, in relation to personal data, means any other person other than an employee of Beyond Psychology who processes data on behalf of Beyond Psychology.

Third Party Third party: means any person other than

- The data subject
- The data controller
- Any processor or other person authorised to process for the data controller

8. PROCESS FOR MONITORING COMPLIANCE

An overall assessment of compliance will take place on an annual basis through completion and publication of the Information Governance Toolkit (IGT), produced by NHS Digital.
Electronic patient record systems will be subject to periodic audit to detect inappropriate access to confidential records.

9. TRAINING

Guidance on confidentiality and data protection will be produced by the clinical director of Beyond Psychology. Training needs will be assessed. All new staff will receive Information Governance awareness training as part of their induction.

10. POLICY PRINCIPLES

Legal requirements exist in relation to the collection, storage, accuracy, retention and disclosure of personal information. All processing of information by Beyond Psychology staff must be carried out in accordance with principles set out in the Data Protection Act and any amending legislation.
While Data Protection legislation applies to living individuals, where possible the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive.

Individuals have certain rights regarding their personal data. These include the right:

- To be informed
- Of subject access
- To rectification
- To erasure
- To restrict processing
- To data portability
- To object
- Not to be subject to automated data processing

Beyond Psychology will ensure that procedures are in place to enable individuals to take advantage of all applicable rights regarding their personal data. In addition to their rights under data protection legislation, individuals have a legal right to respect for private and family life under the Human Rights Act 1998. Beyond Psychology will process personal data and special categories of personal data only where there is a valid legal basis for doing so under GDPR or any equivalent UK legislation. Beyond Psychology will maintain a record of it's processing activities, in a format which complies with requirements set out in GDPR or any equivalent UK legislation.

11. TRANSFER OF PERSONAL DATA

Any transfer of personal data must be carried out securely with an adequate level of protection given to the data in transit in accordance with current Beyond Psychology information security standards. This applies both to the transfer of paper-based information, as well as to data transferred via electronic means, (including email and portable devices such as memory sticks). No personal data may be transferred outside the UK or the European Union without the agreement of Beyond Psychology. Transfers of personal data outside the EU or UK will take place only where the Trust receives assurance that an equivalent level of data protection applies in the receiving country as that provided in the UK. Safeguards must be in place to ensure that personal data is handled, stored and transmitted securely, regardless of the destination.

12. ACCESS TO AND DISCLOSURE OF PERSONAL INFORMATION

Care must be taken to ensure any access to or disclosure of personal or sensitive information is for an authorised purpose. Anyone in doubt as to whether a disclosure of information is authorised should check with their manager.

Data subjects will have a right of access to their information. Requests from patients or their representatives to access their health records must be made in writing. No information relating to patients should be given over the telephone unless the person communicating the information is sure that the person they are speaking to is entitled to receive the information (e.g. a GP Practice).

Personal information will usually be disclosed only if the individual has given their consent to the disclosure. However, under certain circumstances, Beyond Psychology has a power or an obligation to disclose personal information without the individual's consent, (for example to assist the police in preventing or detecting crime, or where a court order is produced). Where Beyond Psychology has a power to disclose information without consent, that power will be exercised only if members of the public, patients or staff are at serious risk.

Requests for information by the police will be considered only where such requests are in the form of a fully completed Data Protection request form. When a decision to release information to the police is made only the minimum necessary information to meet the identified need will be provided. Where the Trust has an obligation to disclose information without consent, (for example, where required by legislation or by a Court Order), such disclosures must be approved in advance by the relevant Director.

13. INFORMATION SHARING

Information will not be shared for purposes beyond direct care where an individual has exercised the right to opt out of sharing information for this purpose, unless there is a mandatory legal requirement or an over-riding public interest in sharing that information.

14. ACCESS TO IT SYSTEMS

Access to systems that hold sensitive or other confidential information relating to clients or staff must be strictly controlled. Beyond Psychology Privacy Policy provides detailed guidance on implementing access control to IT systems. Key standards are:

- Restrict access to a level appropriate to the user's role.
- Access should only be gained by means of a restricted login and, where necessary, a security password or pin number, which is issued when the appropriate training has been received and the relevant level of access has been authorised
- Passwords must be kept secure and never shared with other users. Password sharing is treated seriously and may lead to disciplinary action.
- Users must exit to the appropriate sign-on screen when the computer is not in use.
- No computers should be placed in such a position that unauthorised persons can view patient or other confidential information. If this proves to be impossible, the purchase of a privacy filter should be considered.
- Personal data relating to service users, their families and carers must be processed only on devices issued by Beyond Psychology.

15. INAPPROPRIATE ACCESS TO RECORDS

Access to data for which the member of staff does not have authorisation, at the time the record is accessed, is prohibited. This includes access to his/her own information without a formal request Any staff accessing or attempting to access records they are not authorised to see may be subject to disciplinary procedures. Unauthorised access to or disclosure of information may also render the individual responsible liable to prosecution.

16. STORAGE AND DISPOSAL OF INFORMATION

All printed material containing personal data or confidential organisational information must be treated as confidential and kept secure at all times. Personal data stored electronically must be stored only on devices that have adequate security measures in place. (See Beyond Psychology privacy Policy)

All data (manual and electronic) should be periodically reviewed to ensure that the information is accurate, up to date and complete.

No data (manual and electronic) should be kept for longer than is necessary. Data will be retained in accordance with the retention periods set out in the Records Management Code of Practice for Health and Social Care 2016.

All printed material containing personal data or confidential organisational information must be disposed of securely using the confidential waste disposal service provided by Beyond Psychology.

17. REPORTING BREACHES OF CONFIDENTIALITY

All information governance incidents, including actual and suspected breaches of confidentiality, must be recorded on Beyond Psychology electronic system. Beyond Psychology directors will review each report and if necessary request an investigation by the appropriate department/manager. Where appropriate, an investigation may be deemed to warrant disciplinary action. This will be the responsibility of the line manager.

Where a breach occurs which presents a risk to the confidentiality of a person's data, the data subject will be informed of that breach without undue delay. Where appropriate, breaches will be reported externally to the Information Commissioner.

18. COMPLAINTS ABOUT CONFIDENTIALTY.

Beyond Psychology will deal with complaints about its confidentiality processes within the spirit of Beyond Psychology's Complaints Policy and Procedure. However, complainants also have the right to complain to the Information Commissioner, but usually this is only when the local complaints process has been exhausted.

19. BREACH OF THIS POLICY

Failure to manage personal data securely places Beyond Psychology at risk of breaching data protection legislation. All Beyond Psychology staff have responsibility for the security and proper management of the personal data and other confidential information they process.
Failure to comply with the terms of this and associated policies may lead to disciplinary action and / or legal proceedings against the individuals concerned.

20. REFERENCES

NHS Information Governance - Guidance on Legal and Professional Obligations
Data Protection Act 1998.
General Data Protection Regulation
The common law duty of confidence.
Human Rights Act (1998)
Computer Misuse Act (1990)