Royal College of Occupational Therapists

British Association of Occupational Therapists Ltd

Data Protection Policy

Purpose

The purpose of this policy is to enable the British Association of Occupational Therapists Ltd (BAOT) and the Royal College of Occupational Therapists (RCOT) to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect BAOT /RCOT members, staff and other individuals;
- protect the organisation from the consequences of a breach of its responsibilities.

Data protection is there to ensure that when you are working with personal information it is being done properly.

Scope

This policy applies to:

- the UK office of BAOT / RCOT;
- all staff, whether permanent and temporary and wherever based;
- all volunteers and contractors;
- all branches (regions and specialist section);

All staff are required to read, understand and sign to accept any policies and procedures that relate to the personal data they may handle in the course of their work.

The Law

The Data Protection Act 1998 (DPA) came into force on 1 March 2000 and replaced the 1984 Act. There were also various, subsequent regulations relating to specific topics. The legislation protects the rights of individuals in respect of the data held about them and how that data is then used.

On 25 May 2018 the General Data Protection Regulations (GDPR) came into force which replaced the DPA and which strengthen the rules around personal data. The Data Protection Act 2018 also came into force to consolidate the way in which GDPR is applied locally in the UK.

The Directors of BAOT/RCOT (Council) recognise their ultimate responsibility for ensuring that the organisation complies with its legal obligations.

RCOT has assigned a Data Protection Officer (DPO) who can be contacted at Trevor.White@RCOT.co.uk

The Data Protection Officer has the following responsibilities:

- Briefing Council on its data protection responsibilities
- Reviewing data protection and related policies
- Advising other Boards, Committees and staff on data protection issues
- Ensuring that there is a system in place for data protection induction and training
- Registration with the ICO
- Cooperating with and acting as the contact point for the ICO on issues relating to the processing of personal data
- Handling subject access requests
- Approving all disclosures of personal data
- Approving the wording of contracts with data processors and joint controllers.
- Approving any proposed changes to the use of personal data by a team or department
- Managing the breach reporting process

If you are in any doubt about what you may or may not do, seek advice from your line manager or the Data Protection Officer. In the meantime, do not disclose the information concerned.

BAOT / RCOT take their obligations under GDPR very seriously and any breach of this policy by staff will be handled under RCOT's disciplinary procedures.

Coverage

GDPR covers two key categories of protected information:

1. Personal data

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person

2. Special Category Data

Term	Special categories
Genetic data	Personal data relating to the inherited or acquired genetic characteristics of a natural person
Biometric data (ID Purposes)	Physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person.
Race & Ethnic Origin	Data identifying an individual's racial and/or ethnicity.
Politics & Religion	Personal data relating to political or religious beliefs.
Trade Union membership	Philosophical beliefs, or trade union membership.
Health	The Health and medical records of a natural person.
Sex Life & Orientation	The sexual orientation or sexual practices of a natural person.

Any organisation that collects Personal and/or Special Category Data must comply with the key privacy principles of the GDPR and at least one of the lawful basis for processing.

Key Privacy Principles

The key privacy principles are:

1. Data must be processed in a manner that is lawful, fair and Transparent;
2. Limit your purpose – only collect data for "specified, explicit and legitimate" purposes and no others without consent;
3. Minimise collection – make sure the data collected is accurate and kept up to date;
4. Be Accurate – make sure the data collected is accurate and up to date;
5. Limit storage time – keep data for no longer than necessary and remove data after it is no longer required;
6. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject.
7. Integrity, protection and confidentiality – handle data carefully so as to secure it against loss, damage and destruction.

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

Lawful basis for processing:

1. Consent;
2. Necessary for performance or preparation of a contract with data subject;
3. Necessary for compliance with a legal obligation;
4. Necessary to protect vital interests when consent is not possible;
5. Necessary for performance of public interest task or exercise of vested official authority; and
6. Necessary for purpose of legitimate interests.

Further privacy principles exist for sensitive data which can be found within the GDPR.

Policy Statement

Introduction

BAOT/RCOT regards the lawful and correct treatment of personal information as important to the successful operation of their business and to the maintenance of confidence of those individuals with whom they deal. Both organisations will ensure that their staff and those acting on their behalf obtain, use and disclose personal information lawfully and correctly.

BAOT/RCOT recognises that their priority under the GDPR is to avoid causing harm to individuals. Consequently, they will keep personal data secure by:

- complying with both the GDPR's and good practice;
- respecting individuals' rights;
- being open and honest with individuals whose data are held;
- providing training and support for staff who handle personal data so that they can act confidently and consistently.
- implementing appropriate security measures to protect personal data in storage, use and in transit.

This statement sets out BAOT / RCOT's approach to data protection and outlines the responsibilities of staff (employees, volunteers, contractors) in complying with the principles set out in the GDPR. Any questions or concerns about the interpretation or operation of this statement should be taken up in the first instance with the Data Protection Officer.

Any employee who considers that the GDPR has not been followed in respect of themselves as employees or who is concerned that there is a breach of the GDPR should complete a Data Breach Notification Form and send this to the Data Protection Officer.

Processing personal data

There are 8 rights of Data Subjects under the GDPR's regulations to ensure that individuals' data is handled correctly. BAOT / RCOT both adhere to these which are **the right**:

1) to be informed;
2) to access their data;
3) of rectification of their data;
4) to make their data portable;
5) to erasure;
6) to restrict or block data processing;
7) to object to having their data process; and
8) to be protected from automated decision making processes.

There principles can be summarised into some basic 'do's and don'ts' regarding processing personal data in BAOT /RCOT:

Do:

- **be clear that the information being collected is lawful**
- **explain why the information is being collected**
- **keep the information as accurate and up-to-date as possible**
- **destroy it when it is no longer required**
- **remember that individuals have the right to access their information at any time**
- **keep it secure at all times**

Don't:

- **use the information for any unrelated purpose than that originally specified**
- **collect or process information not directly relevant to the specified purpose**
- **save any information on to portable storage devices**
- **disclose information to third parties unless you are confident that the disclosure is permitted.**

Access to Personal Data ("Subject Access Requests")

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request the Data Controller must provide a copy of all the personal data about that individual held at the time the application was made. The request must be dealt with within 30 days of receipt of the request, unless the request is unreasonable.

Policy reference Links:

Data Breach Notification Form: http://phoenix/phoenix/GDPR/index.php