Data Protection Policy

Aims

The company needs to keep certain information on staff and applicants in order to lawfully carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the aims of GDPR. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organization, including the use of IT equipment and software.

This policy covers staff, volunteers and also subcontractors.

Definitions

In line with the principles of GDPR, The company will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The GDPR includes the following rights for Individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

For the purposes of International trade, our lead data protection supervisory authority is the ICO in the UK.

Notification

We are exempt from being listed on the public register maintained by the Information Commissioner. We review this on an annual basis as the law requires.

The name of the Data Protection Officer within our organisation as specified in our notification to the Information Commissioner is Richard Curtis.

Responsibilities

All staff who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy or unauthorised disclosure may result in disciplinary or legal action being taken.

Data Protection Impact Assessments

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

These will be undertaken by the development team with the Data Controller.

If a DPIA indicates that the data processing is high risk, and the company cannot sufficiently address those risks, the Data Protection Officer will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Implementation

To meet our responsibilities all staff will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information will be given this policy and trained to handle the data.
- Staff are given annual refreshers of their data protection responsibilities and malware identification training (and more frequently if a risk is identified);
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.

Queries about handling personal information will be dealt with swiftly and politely.

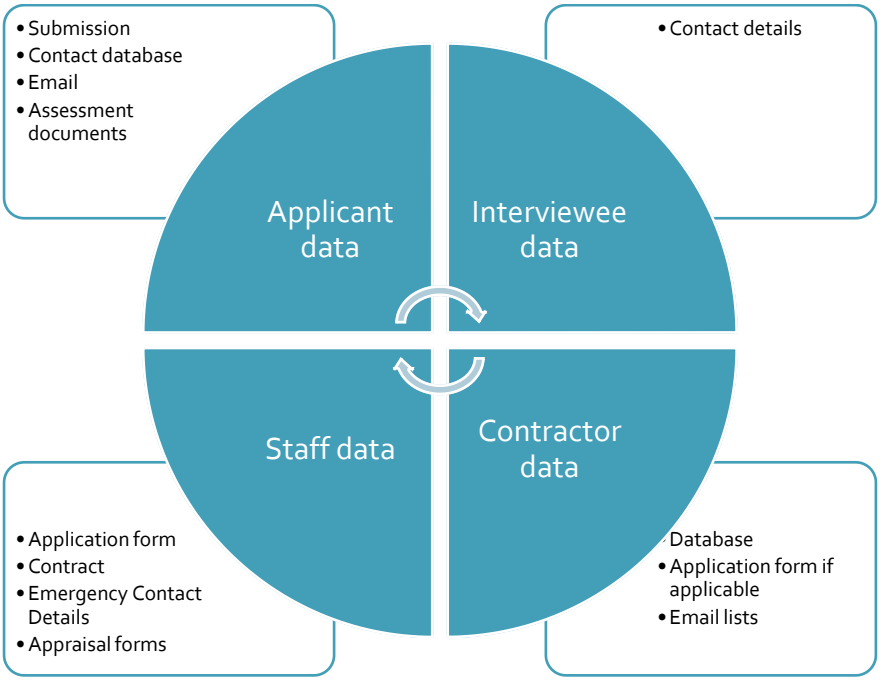
Gathering and checking information

Before personal information is collected, we will consider if it needs to be collected and for what lawful purpose. We will inform clients whose information is gathered. We will ensure that these records are kept up to date. Personal sensitive information will not be used apart from the exact purpose for which permission was given.

When people request information from our automated system, they receive an email to confirm they want to receive information from us, which is logged on our system. People contacting us by

email or phone will be giving implied consent to be contacted in relation to their enquiry. Before receiving other marketing communications, their permission will be sought.

Personal data held and processed by the company



Data Storage

The company operates predominantly online, consisting of:

- Main websites
- OneDrive storage

All online sites are stored and backed up on EU based servers.

The company uses Microsoft Office 365 for email and OneDrive for data files, which are also stored locally on a computer and backed up to an off-site backup system. This enables the company to be able to guarantee data access from one of the three storage points at any time.

Data access

Only authorised persons are allowed to access personal data. The company uses Microsoft OneDrive to store the majority of our data (explained above). Access privileges are authorised on a per user basis by the CEO and users are verified members of staff (i.e. their identity has been confirmed during their recruitment process).

Data sharing

Data is collected from applicants to apply for the accreditation. Predominantly assessors are internal members of staff, however there may be occasions that we use an external contractor. These contractors are required to comply with our data protection policy and this policy.

Data transmission

Personal data is transmitted using secure methods, such as temporarily sharing online access to files for the purpose of the accreditation. They are not able to download copies of the files and access is only allowed for the period of the assessment.

Data breaches

The company keeps data secure and monitors routinely for data breaches. In the event of a data breach that results in a high risk to the rights and freedoms of Individuals, the company will report the breach to the ICO within 72 hours (ideally within 24 hours). They will also inform the Individuals affected.

Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to Richard Curtis, The Mental Health Tick, 3 Merridale Road, Southampton, SO19 7AB.

Queries about handling personal information will be dealt with swiftly and politely. The company have the right to refuse or charge for requests that are manifestly unfounded or excessive. If a request is refused we will inform the Individual of the reason within 30 days, the Individual retains the right to complain to the ICO.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 30 days required by the GDPR from receiving the written request and relevant fee.

Right to be forgotten

Anyone whose data we hold has a right to be forgotten. Individuals seeking to use their Right to be Forgotten, should email richardc@mentalhealthtick.com with a form of ID to allow our staff to

verify their identity. Once this is confirmed our staff will remove the records held on our online resource site(s) and email systems within 14 days.

Review

This policy will be reviewed biannually by the CEO.

January 2021