



Data protection policy

Principle:

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our clients. We recognise the need to treat it in an appropriate and lawful manner.

Threecm has a professional duty to comply with relevant legislation governing the complex issue of data protection including the Data Protection Act 1998 (DPA) and guidance provided by the Information Commissioners Office (ICO), Department of Health and other relevant bodies.

It is the responsibility of each individual case manager to ensure they are familiar with the relevant legislation and guidance when dealing with person identifiable data.

This policy applies to computerised processing of personal data as well as paper-based files.

Standard 1:

1.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

1.2 Fair and lawful processing

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, the purpose for which the

data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

1.3 Processing for limited purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

1.4 Adequate, relevant and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

1.5 Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

1.6 Timely processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

1.7 Processing in line with data subject's rights

Data must be processed in line with data subjects' rights.

Data subjects have a right to:

Request access to any data held about them by a data controller.

Prevent the processing of their data for direct-marketing purposes.

Ask to have inaccurate data amended.

Prevent processing that is likely to cause damage or distress to themselves or anyone else.

1.8 Data security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

1.8 Dealing with subject access requests

A formal request from a data subject for information that we hold about them must be made in writing.

Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular, they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Refer to their Manager/Employer for assistance in difficult situations. No-one should be bullied into disclosing personal information.

Standard 2:

2.1 All Threecm case managers will be registered with the ICO as standard in order to handle personal data defined as:

2.2 Personal data

The Data Protection Act 1998 defines personal data as that which relates to a living individual who:

- can be identified from that data or
- from that data and any other information which is in the possession of, or likely to
- come into the possession of, the data controller and includes any expression of opinion about the individual and any intention of the data
- controller or any other person in respect of the individual.

2.3 Definition of data

Data is defined as information which is:

- processed automatically or recorded with the intention to process automatically, or
- recorded as, or with the intention that it be, part of a manual "relevant filing system"
- which is further defined in the Act or
- contained in a health, educational or social services record.

Threecm policy: reviewed November 2017

Next review: November 2018