Matrix College of Counselling and Psychotherapy

Data protection policy

INTRODUCTION

1.1 The way in which Matrix College ("Matrix" or "the College") uses personal data is regulated by applicable data protection legislation, meaning the Data Protection Act 2018, and, for the period it remains in force in the UK, the General Data Protection Regulation (EU) 2016/679 and any other applicable laws relating to the protection of personal data and the privacy of individuals (all as amended, updated or re-enacted from time to time).

1.2 The Director and Administrator have day to day responsibility within the College to ensure that data protection best practice is implemented and observed.

1.3 The Management Team approves this policy in accordance with the approval of policies system at the College

2 SCOPE

2.1 Matrix recognises that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful future growth, development and operation. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.

2.2 Matrix understands that in the event personal data is mishandled, the College may be exposed to potential fines of up to €20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher.

2.3 It is important for everyone within the College to understand the principles of the data protection legislation, so as to enable Matrix to comply with its obligations. This policy sets out the responsibilities of anyone who processes personal data on behalf of Matrix, including officers, consultants, full- and part-time employees, contractors and any other third parties.

2.4 Any questions or concerns about the interpretation or operation of this policy should be addressed to the Administrator

3 SHORT GUIDE TO DATA PROTECTION LEGISLATION

3.1 What is "personal data"?

3.1.1 Personal data is information relating to a living, identifiable individual (a "data subject"). A person is sufficiently identifiable by the College if they can be 'singled out' within a given environment, including online, either from a given set of data we hold, or where we could do so by combining different data sets the College possesses or can reasonably access. A person can be 'singled out' even if we do not know their name.

3.1.2 Matrix processes personal data relating to a number of categories of data subject, including employees, tutors, students, applicants, CPD event attendees business contacts, visitors, suppliers and contractors. For example, personal data includes names, addresses, email addresses and telephone numbers; it may also include images caught on CCTV cameras and recorded telephone conversations.

3.1.3 Personal data is not always factual; it can also include opinions expressed by one person about another.

3.1.4 Data protection legislation applies to all formats of information including information stored on computers and in certain manual (for example, paper) filing systems, provided that they are structured in a way that enables easy access to information about a data subject.

3.1.5 There is a sub-set of personal data called "special categories of personal data" which is information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric and genetic data. Special protection is also given to personal data relating to criminal offences and convictions. Data protection legislation prohibits the processing of this more sensitive and private data except in specific circumstances.

3.2 What does "processing" personal data mean?

3.2.1 Processing has a broad definition and includes almost anything Matrix might do with personal data, including obtaining, recording, holding, using, disclosing and destroying personal data.

3.3 What can we do with personal data?

3.3.1 We need to process personal data lawfully, fairly and transparently. The data protection legislation sets out the list of lawful justifications for processing - often referred to as the "conditions for processing" and there is an explicit obligation to tell data subjects the legal basis for processing their personal data.

3.3.2 The choice of lawful basis depends on the purpose or reason for which we are collecting or using the personal data, and the lawful basis we identify then has implications – it affects the extent to which the data subject can limit our use of that data, or even whether they can require us to delete it entirely. Information on data subject rights is included in Section 5 below.

3.4 What are "data controllers" and "data processors"?

3.4.1 A "data controller" determines the purposes for which and the manner in which personal data are processed. Matrix is a data controller in respect of personal data it holds relating to staff. It is also a data controller in respect of certain personal data it holds relating to students and staff (e.g. where the data is used to send billing or marketing information or to comply with legal or obligations relating to fitness to study processes).

3.4.2 A “data processor” is any person (not an employee of the data controller) who processes data on behalf of the data controller, for example agents and contractors. Data controllers do not make decisions about how and why data is to be processed – they instead implement the instructions of the data controller.

3.4.3 A data controller remains responsible for the use of information by a data processor in respect of information it has passed to the data processor and we must take steps to ensure that these processors are able to protect personal data before providing it. Matrix is required to put in place a written contract with any data processors. Anyone wishing to appoint a data processor should first speak to the Director

3.5 What must staff do to comply?

3.5.1 We will adhere to the following principles relating to processing of personal data:

Principle	Requirement and what we will do

Lawfulness, fairness and transparency	• Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
	  ○ We provide the data subject with information about his/her personal data processing in a concise, transparent and intelligible manner, which is easily accessible, using clear and plain language.
	  ○ If we need to transfer personal data outside of the EEA, we ensure that it is adequately protected in accordance with legal requirements.

Purpose limitation	• Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. ○ We regularly review the purposes for which we use personal data and will take steps to inform the data subject in advance of any changes to those purposes.
Data minimisation	• Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. ○ We ensure that we collect enough data to achieve our purposes but not more than needed.
Accuracy	• Personal data shall be accurate and, where necessary, kept up to date. ○ We take reasonable steps to delete or amend inaccurate or outdated data.
Storage limitation	• Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. ○ We ensure that data is kept for no longer than necessary, and have in place an archiving policy and review this process annually.

Integrity and confidentiality	• Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
	  ○ We assess risk, implement appropriate security for personal data and check on a regular basis that it is up to date and working effectively.
	  ○ All data processors appointed by Matrix are assessed against their ability to adequately protect personal data and we have formal agreements in place with them.

Accountability	• Matrix is responsible for, and must be able to demonstrate compliance with, data protection legislation ○ We maintain records of our compliance and

	undertake periodic audits to ensure we continually improve our processes and measures to protect personal data

3.6 Anyone who is unsure whether they are authorised to collect or disclose personal data in a certain way should check with the Director In particular, if anyone (including the Police, other officials, or even the spouse of the data subject) requests access to personal data relating to a data subject, staff must first check with their line manager or the Director before making any disclosure.

3.7 Data subjects are entitled to ask Matrix to provide a copy of any information that Matrix holds about them. Accordingly, Matrix should not keep on record any information, opinion or judgement which Matrix would not want to show to the data subject or explain or justify if called upon to do so.

3.8 Matrix will provide further training to staff in their responsibilities in respect of personal data, and staff should take up these training opportunities.

4 THE RIGHTS OF DATA SUBJECTS

4.1 Data subjects also have a range of rights in relation to their personal data and how we process it, namely:

4.1.1 the right to be informed of various information about how their data is being used and why;

4.1.2 the right to receive an copy of data they have provided to us, and to have certain data transmitted to another data controller

4.1.3 the right to have any inaccuracies in their data corrected, which may include the right to have any incomplete data completed;

4.1.4 the right to have their personal data erased in certain circumstances;

4.1.5 the right to have the processing of their data suspended, for example if they want us to establish the accuracy of the data we are processing.

4.1.6 the right to object to any direct marketing (for example, email marketing or phone calls) by us, and to require us to stop such marketing.

4.1.7 the right to object to the processing of their information in situations where we are processing that data based on the lawful bases known as ‘legitimate interests’ or ‘public task’; and

4.1.8 the right to object to any automated decision-making about them which produces legal effects or otherwise significantly affects them.

4.2 Requests can be made by any channel (email, letter, over the phone, even via social media). We must respond within 1 month.

4.3 If an employee receives a communication from any individual, which appears to be attempting to exercise one of the above rights, it should be immediately forwarded to the Director

5 RISKS TO MATRIX OF BREACHING DATA PROTECTION LEGISLATION

5.1 Besides the power to impose fines up to €20million, the Information Commissioner's Office ("ICO") has a range of corrective powers and sanctions to enforce data protection legislation. These include issuing warnings and reprimands; imposing a temporary or permanent ban on data processing; ordering the rectification, restriction or erasure of data; and suspending data transfers to third countries.

5.2 An individual affected may ask the ICO to assess whether an organisation's processing of personal data is being undertaken lawfully. If that occurs, the ICO is required to make an assessment as to whether data protection legislation has been breached.

6 INFORMATION SECURITY

6.1 Matrix has an obligation to ensure that any personal data we hold is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

6.1.1 Matrix shall ensure that personal data is stored securely using modern software that is kept-up-to-date. In particular, software updates issued by the software providers are to be implemented within a short period of their publication.

6.1.2 Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

6.1.3 When personal data is deleted this should be done safely such that the data is irrecoverable. Hardware is to be disposed of securely, only after and data has been erased.

6.1.4 Appropriate back-up and disaster recovery solutions shall be in place.

6.2 Every member of staff has a responsibility to enable Matrix to comply with this obligation.

7 REPORTING DATA BREACHES

7.1 A personal data breach is "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*". This includes breaches that are the result of both accidental and deliberate causes.

7.2 Common examples of data breaches are:

7.2.1 emailing and/or posting personal data to incorrect recipients; and

7.2.2 leaving personal data in unsecure locations.

7.3 You must report any actual or suspected information security incident/ data breach to the Director immediately upon discovery. Under the current legislation, Matrix may need to notify the ICO within 72 hours of your discovery of the breach, and may need to take swift action to mitigate any potential detriment. Delay in reporting the issue internally may prevent Matrix from complying with its statutory obligations.

8 HANDLING REQUESTS FOR ACCESS TO DATA BY DATA SUBJECTS

8.1 Data protection legislation gives individuals the right to know what information is held about them. This right only allows access to the requestor's own personal data (with some permissible exceptions).

8.2 If an individual requests a copy of their personal data, whether verbally or in writing, staff should immediately pass that request on to the Director

8.3 Under the current legislation, Matrix has one calendar month to respond to the request. Matrix may be able to extend the period of compliance by a further two months where requests are complex or numerous. If so, the College must inform the individual within one month and explain why.

8.4 On receipt of a request, Matrix will formally confirm receipt to the requestor. Matrix may request proof of identity form the requestor.

8.5 Matrix will then conduct a reasonable and proportionate search for relevant material and will disclose the data it contains to the requestor, save to the extent that exemptions under data protection legislation apply.

9 GUIDANCE FOR STAFF ON THE USE OF THEIR PERSONAL DATA

9.1 Matrix will process the personal data of our members of staff in accordance with this policy and as set out in the employee privacy notice and contracts of members of staff.

9.2 It is the responsibility of each individual member of staff to:

9.2.1 check that any information that they provide in connection with their employment is accurate and up-to-date;

9.2.2 inform Matrix of any changes to information which they have provided e.g. change of address; and

9.2.3 inform Matrix of any errors or changes.

9.3 Matrix may publish the names, work telephone numbers and work email addresses of our members of staff on the College website, unless the members of staff give notice that they do not wish this to happen.

10 GIVING REFERENCES

10.1 Nobody should give references in respect of current or past employees of Matrix without prior approval of the Director. Requests for references should be passed to the Director in the first instance. A copy of any reference given should be retained in the staff member's employment record.

10.2 All references (whether oral or written) given in respect of a student at Matrix should contain only information that is factual or is an honest opinion or judgement that is capable of being demonstrated as being reasonable by reference to actions or events. Copies must be provided to the College for storage on the relevant student file.

10.3 Referees should be aware that the content of a reference may, at a future date, be shared with the individual concerned.

Developed by: Management team
Date: November 2019
Due for review: June 2020