Marjon Counselling Clinic
Policies and Procedures

PLYMOUTH MARJON UNIVERSITY

MARJON HEALTH & WELLBEING

Confidentiality, Data Protection and Information Sharing

The MCC's Confidentiality, Data Protection and Information Sharing Policy aims to align with the following polices:

- The BACP Ethical Framework (incl. Good Practice in Action [GPiA] on "Managing Confidentiality within the Counselling Professions",
- "Safeguarding Vulnerable Adults within the Counselling Professions and "Record Keeping within Organisational Settings in the Counselling Professions"
- The PACH05/PACMO1 Placement Agreement
- The PMU WBPL Policy
- PMU Data Protection Policy

Confidentiality

Introduction

The MCC offers the highest level of confidentiality to its clients consistent with the Ethical Framework of BACP and with the law. This involves adherence to common law, statutory provisions and regulations (e.g., the United Kingdom General Data Protection Regulation (UK-GDPR), Data Protection Act 2018, Freedom of Information Act 2000, Human Rights Act 1998 Article 8), and the contractual agreement between the client and the clinic.

For the purpose of this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organisations (confidential information), which comes into the possession of the organisation through its work.

The MCC holds personal data about its staff and clients which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of the organisation without prior permission. All personal data will be dealt with sensitively and in the strictest confidence internally and externally.

Purpose

The purpose of the Confidentiality Policy is to ensure that all clinic staff, students and clients understand the clinic's requirements in relation to the disclosure of personal data and confidential information.

Limits to Confidentiality

No information given to the MCC will be shared with any other organisation or individual without the user's expressed permission.

However, the MCC recognises that occasions may arise where individual clinic staff or students feel they need to breach confidentiality. Confidential or sensitive information relating to an individual may be divulged:

- to assist in the prevention or detection of a serious crime.

- where a risk of danger to the individual, a staff member or student, or the public at large is present.

- where there are statutory obligations to disclose information (e.g. The Terrorism Act 2000, Drug Trafficking Act 1994, Proceeds of Crime Act 2002 and the Money Laundering Regulations 2007). In these circumstances, information may be divulged to external agencies e.g. police or social services on a need-to-know basis.

- where a court orders disclosure of documents or information relating to client work.

Where a student or the Clinic Manager/Deputy feels that confidentiality should be breached, safeguarding procedures should be followed, as per the **MCC Safeguarding Policy.**

When considering a breach to confidentiality due to a Safeguarding concern, students and client staff should review the following:

- The MCC recognises that we must contribute to inter-agency working in line with statutory guidance and legislation and share information between professionals and agencies where there are concerns to safeguard children and adults at risk.
- All members of the university must be aware that they have a responsibility to share safeguarding concerns with appropriate agencies or individuals, and that the Data Protection Act 2018 is not a barrier to sharing information where the failure to do so would place an adult at risk or a child at risk of harm.
- All MCC staff and students must be aware that they cannot promise confidentiality to a child or adult at risk where this might compromise the wellbeing or safety of them or others.
- The MCC recognises that all matters relating to safeguarding are personal to the individuals and families involved. Therefore, this information will be treated with the utmost sensitivity and the Clinic Manager/Deputy will only disclose it on a 'need to know' basis.
- Records of all information relating to safeguarding concerns will be held securely, and access to this information will be held only by the Clinic Manager/Deputy and the client's Student Counsellor. Should there be a need for individuals other than the Clinic Manager/Deputy and Student Counsellor to access this information, it will be anonymised where possible to protect the identities of those concerned.

Our student counsellors also receive supervision on all their counselling work; the supervision itself is kept confidential. **Counsellors will not use clients' names during supervision.**

(*Supervision means that a counsellor uses the services of a Qualified Clinical Supervisor to review their work with clients).*

Ensuring the Effectiveness of the Policy

All clinic staff and students will be introduced to the confidentiality policy via induction. Student Counsellors will also undertake mandatory Confidentiality and GDPR online training before starting placement in the clinic. The policy will be reviewed annually, and amendments will be proposed and agreed to by the Clinic Manager.

Non-Adherence

Breaches of this policy will be dealt with according to the MCC Code of Conduct Policy, the SRF and PMU Data Protection Policy.

Further Information

We will always endeavour to **discuss any changes of boundaries of confidentiality** with clients. However, this may not be possible in certain situations, for example in cases of terrorism, certain child protection situations (such as where it may be dangerous to a child or others to alert a person about impending disclosure or may compromise a police investigation) or mental incapacity.

No-one outside the counselling clinic and need know that clients have utilised our services, unless they choose otherwise. Please note that Marjon University is a campus University, therefore it is likely that people will be on campus during sessions.

Communication outside session is at the discretion of the client's preference; however, unless discussed, counsellors will not make it apparent that the client is known to them.

<u>Data Protection and Information Sharing</u>

Introduction

The MCC commits to keeping accurate records that:

• are adequate, relevant and limited to what is necessary for the type of service being provided.

• comply with the applicable data protection requirements, see www.ico.org.uk.

What type of information does the clinic hold?

The clinic currently collects and processes the following information:

- Personal identifiers, contacts and characteristics (for example, name and contact details)

- Demographic details
- Emergency contact details for safeguarding practice
- Assessment notes

How we receive information and why we hold it

Most of the personal information we process is provided to us directly by our clients for one of the following reasons:

- To understand what has brought you to counselling and how we can best support you.
- To fulfil our requirements under our safeguarding policy.
- To fulfil our requirements under our equal opportunities and diversity policies.

Under the General Data Protection Regulation (GDPR), the lawful bases which the clinic relies on for processing this information:

(a) The clients consent. A client can remove their consent at any time. They can do this by contacting the Clinic Manager.

(b) A contractual obligation.

(c) The clinic keeps records for a minimum of 3 years post the completion of our work with a client in case of complaint or claims. After this point, electronic information will be securely deleted.

(d) We have a legitimate interest.

How the clinic uses information

The clinic uses the information that has been provided by clients in order to understand client needs and how we can best support them. We this information to clients to a counsellor that will be suited to the support that the client requires.

The clinic may share this information if a risk has been reported. Due to our safeguarding policies, we will breach confidentiality if a client makes a member of the clinic team aware of an imminent risk to your life or another, or a crime in progress. The Clinic Manager may share information with a client's emergency contact, other agency bodies, or the police if a serious risk has been reported/ in progress.

Outcome Measures

The clinic routinely collects information on the counselling service and our clients to enable us to continually evaluate and develop the provision. Throughout counselling, clients will be asked to complete questionnaires via an online link. These questionnaires will also help us to keep track on client progress and improvement during counselling. Anonymised client data will also be used to contribute to clinic-wide support research at Marjon. Clients have the option to opt of out of having their data used in clinic-wide research, prior to data anonymisation taking place. This decision will not affect their access to the service. Clients will be included in research unless they explicitly choose to opt out. All data will be held as part of your client record on the secure client database, or on the universities secure network.

The clinic may ask clients if they would like to be approached as a potential participant in further clinic or student research projects. If you agree to be approached, any projects you are invited to participate in will be fully explained to you and you are free to decide whether this is something you want to be involved in. All research conducted at the clinic will be led or supervised by researchers and academic staff of the University and is subject to ethical approval from the Plymouth Marjon University Ethics Committee.

How the clinic stores client information

Principles

• All personal paper-based and electronic data must be stored in accordance with the Data Protection Act 1998 and must be secured against unauthorised access, accidental disclosure, loss or destruction.
• All personal paper-based and electronic data must only be accessible to those individuals authorised to have access.

The clinic strives to be a paperless whenever feasible. Hence, all client records are kept on secure, password protected clinic management software, and/or on the universities secure network, on password protected laptops. In cases where it is not possible to input client data directly into the clinic management software due to platform restrictions, the information will first be added to the university's secure, password-protected database. Subsequently, and where possible, it will be promptly transferred to the Clinics Management Software.
If any information is gathered via paper, it will be immediately scanned and uploaded to the client database(s). Any paper copies will then be destroyed by shredding and disposed of in confidential waste collections.

In the unlikely event where a serious data breach has occurred, the Clinic Manager/Deputy will notify the ICO about any breaches which may pose a real and serious risk to the rights and freedoms of individuals.

Information Sharing

The clinic may also receive personal information indirectly, from the following sources in the following scenarios:

- Agencies may refer clients to the MCC for help and support. Client information is provided to ensure we understand what has brought clients to counselling and how the clinic can best support them, to fulfil our requirements under the clinics safeguarding policy, and to fulfil the clinics requirements under our equal opportunities and diversity policies.

- With a client's consent, the clinic may share personal information with other organisations or agencies for help and support.

When sharing information is necessary and/or appropriate, the clinic will limit the information disclosed to the minimum necessary in order to avert risk. The Clinic Manager/Deputy will also make a note as soon as possible of the following:

- The date of providing the information
- To whom the information is given
- The content of the information shared
- The method of disclosure or referral
- Whether consent was given (and by whom)
- If the disclosure is made without consent, the reasons why this decision was made will be recorded

Client data protection rights

Under data protection law, clients have the following rights:

Right of access - Clients have the right to ask the clinic for copies of their personal information.

Right to rectification - Clients have the right to ask the clinic to rectify information they think is inaccurate. They also have the right to ask the clinic to complete information they think is incomplete.

Rright to erasure – Clients have the right to ask the clinic to erase their personal information in certain circumstances.

Right to restriction of processing - Clients have the right to ask the clinic to restrict the processing of their information in certain circumstances.

Right to object to processing - Clients have the right to object to the processing of their personal data in certain circumstances.

Right to data portability - Clients have the right to ask that the clinic transfers the information they gave us to another organisation, or to themselves, in certain circumstances.

Clients are not required to pay any charge for exercising their rights. If clients make a request, the clinic has one month to respond.

Please contact the Clinic Manager/Deputy if you wish to make a request. A request form will be sent to you to complete. Once this is received back, we will fulfil your request within 1 month.

How to Complain

Clients have the right to complain if they feel unhappy with how the clinic has processed or kept their information. The MCC takes any complaint seriously and will investigate the matter thoroughly. See the MCC Complaints Policy for information on how to make a complaint.

Clients can also complain to the ICO if they are unhappy with how the clinic has used their data.

ICO webpage: https://ico.org.uk/

ICO helpline number: 0303 123 1113