# Data Protection & Information Sharing Policy

**Reviewed & Updated by:** Charis Bull

**Date approved by the Board of Trustees:** December 2013

**Review Date:** December 2015

## Overview

*Application of this policy will be on the basis of equal opportunities regardless of race, colour, nationality, or ethnic origins, age, marital status, gender, sexual orientation, disability, religion or other personal circumstances or disadvantages.*

This Data Protection Policy describes the way that the Brighton Oasis Project will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998 as that is the key piece of legislation covering security and confidentiality of personal information.

# Contents

## Legislative Framework

Common Law Duty of Confidence
Children's Act 1989
Computer Misuse Act 1990
Data Protection Act 1998
Human Rights Act 1998
Crime and Disorder Act 1998
The Protection of Children Act 1999
Terrorism Act 2000
Freedom of Information Act 2000
Health & Social Care Act 2001
Sexual Offences Act 2003

## National Guidance and Local Protocols

South East Coast Overarching Information Sharing Protocol
Confidentiality: NHS Code of Practice 2003
NTA – Confidentiality and Information Sharing 2013

## Other Relevant Policies/ Procedures/ Guidelines

Confidentiality Policy
Safeguarding Children Policy
Staff Code of Conduct
Third Party Reporting Protocol

## Scope of Policy

- This policy applies to all BOP management, employees, volunteers, and service users.
- This policy is applicable both on and off premises during BOP-related activities.

## Policy Statement

The Brighton Oasis Project needs to collect and use information about individuals with whom it works in order to operate and carry out its functions effectively. These may include current, past, and prospective service users, employees, and volunteers (data subjects). In addition the organisation is required to collect and share certain information in order to comply with the requirements of the National Treatment Agency (NTA).

Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. The Brighton Oasis Project regards the lawful and appropriate treatment of all personal information as crucial to successful service delivery and essential to maintaining confidence between the organisation and those individuals who are involved with it. The organisation therefore fully endorses and adheres to the Principles of the Data Protection Act 1998.

Government policy however allows agencies to work across boundaries to provide services on a multi-agency basis according to the needs of service users. Essential information must, therefore, be able to pass between the Substance Misuse Services, NHS, Local Authority, Social Services and other services (such as housing, youth offending team, education, voluntary or independent bodies) where those organisations are contributing to, or planning, a programme of care, or where one may need to be initiated. The balance between the need to share information to provide quality service and protection of confidentiality is often a difficult one to achieve. This policy, in conjunction with the South East Coast Overarching Information Sharing Protocol (2013) and our Safeguarding Children and Confidentiality Policies, aims to clarify and guide this balance.

# Relevant Procedures & Implementation Guidelines

## 1. Training & Dissemination of Information

All employees will be made aware at induction of their responsibilities under the terms of this policy and the Data Protection Act, including reasonable precautions necessary to securely record and share data.

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

Service users will be informed of our duties under the Data Protection Act 1998 as part of their induction onto a day programme and a signed consent form to share information will be kept with their file.

## 2. Advice & Consultancy

Where reasonably practical all relevant staff will be consulted on modifications and updates to procedures relating to data protection and information sharing.

The following agencies could also be consulted on specific confidentiality and information sharing matters:

The Information Commissioners Office

## 3. Employee Contracts

Each employee will sign a confidentiality (non-disclosure) undertaking as part of their contract of employment and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any personal data, however it is stored. Employees should also be mindful of their professional code of conduct (FDAP – see **Appendix B**) or the codes of conduct from other professions that they are aligned to (such as Social Work or Nursing). Failure to comply will result in the instigation of a disciplinary procedure.

## 4. Data Protection Act 1998

The Data Protection Act 1998 became law in March 2000 and covers personal information about living individuals that is held in any media e.g. paper files, computer records, audio and video tape, etc.

The Act is implemented by abiding by eight principles. There are penalties both civil and criminal within this Act and individuals as well as organisations can face action through the court for breaches of these. These principles are defined below and are summarised again in **Appendix A**.

### I. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully

Brighton Oasis Project can process personal data where one of the following conditions has been met:

- The data subject has consented to the processing
- Processing is necessary for the performance of a contract with the data subject
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the data subject

All data subjects are to be made aware that Brighton Oasis Project processes data, the identity of the data controller (the Director), the purposes for which the data will be processed and the likely consequences of the processing and how data is shared.

All data subjects of Brighton Oasis Project must give their explicit consent for the gathering and processing of sensitive data unless the processing is required by law for employment purposes or for administration of justice or legal proceedings or to protect the vital interests of the data subject (e.g. in a child protection case). See section 7 within this policy and/or the Confidentiality Policy for further information on this.

Sensitive data includes their racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexuality or criminal proceedings or convictions. Any non-routine disclosure of information must be approved by the Director who is the Designated Information Officer. Non-routine disclosure requests for which there is no legislative requirement to share information, for example, reference requests for clients by commercial companies will only be authorised by the Designated Information Officer if the client has given explicit consent, in consultation with the client if appropriate, and only in circumstances where the client would not be adversely affected by so doing.

All data subjects have the right to refuse consent to process their data.
If a subject withholds consent to process their personal data, this will be respected, but it may mean that we are unable to work with the subject, and in the case of an employee or volunteer, they would be unable to take up a position with the organisation.

See sections 6 and 7 for further information about this.

## II. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or purposes

All client records should follow the following guidance:

- Always date and sign/initial records.
- Record information as soon after the contact as possible to maintain high levels of accuracy.
- Record in a style that is legible, able to be photocopied, and cannot be easily changed or deleted.

- Changes/modifications of records should be dated and signed.
- Do not include jargon or abbreviations.
- Do not include irrelevant information.
- Clearly differentiate between matters of fact and opinion.
- Do not express opinions that you are not prepared to defend, or which you cannot substantiate.
- Do not express opinions in areas where you are not qualified.
- Always be sure of the facts.
- Do not write in anger or in haste. This is particular danger with e-mails because of the immediacy of e-mail as a means of communication.
- Always speak respectfully of the person, even when expressing negative information.

## III. Personal data shall be accurate and, where necessary kept up to date

All active client records will be reviewed on a three-monthly basis and updated - any mistakes identified will be corrected. Any inactive client files will be securely stored, and will be securely destroyed after a period of time as outlined under section VI below.

## IV. Personal data shall be processed in accordance with the rights of the individual under this Act

An individual shall be entitled at reasonable intervals and without undue delay or expense:

- To be informed by any data user whether he or she holds personal data of which the individual is the subject, and
- To access any such data held by the data user, and
- Where appropriate to have such data corrected or erased

The Brighton Oasis Project operates an ‘open file’ policy where service users have the right to access any person-identifiable information that is held about them at BOP. This will be made available to the subject within three weeks of receiving a written request to see it. A certain editorial process may omit details made available to the service user under the grounds that it may cause serious harm to their (or others) mental or physical state, or that it contains information about a third party. Any information sent to a third party about a subject will similarly be made available to them after receiving a written request and a small processing fee. See the NHS guidance on Access to Health Records in the references section for more information on this. Clients should be made aware of their rights about this at induction.

## V. Personal data shall be obtained only for one or more specified lawful purpose(s). Personal data held for any purpose or purposes

## shall not be further used or disclosed in any manner incompatible with that purpose or purposes

We will only collect data for a specific purpose and in relation to clients - in order to best meet their needs. See sections 6, 7, & 8 for further information about disclosure of information incompatible with the purpose for which it was obtained.

## VI. Personal data held for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes

At the Brighton Oasis Project files are kept for a certain period of time in accordance with NHS best practice:

| **Type of Record – Service Users** | **Duration of Retention** |
|---|---|
| Adult service user files (inactive) | 3 years after conclusion of treatment |
| Adult service user files with mental health diagnosis (inactive) | 20 years after conclusion of treatment (or 8 years after death) |
| Children and Young People's records (under 18s) | Until their 25th birthday (or 26th if they were 17 at the conclusion of treatment) |
| **Type of Record – Employees / Applicants** | **Duration of Retention** |
| Unsuccessful recruitment candidates not shortlisted | 4 months from date of advice |
| Unsuccessful recruitment candidates shortlisted but not selected | 4 months from date of appointment |
| References received | 1 year |
| Annual Leave records | 2 years |
| Sickness records | 3 years |
| Unpaid / Special Leave records | 3 years |
| Annual Appraisal / Assessment Records | 5 years |
| Payroll and Tax Information | 6 years |
| Records relating to accident or injury at work | 1 year from end of employment |
| Application form | Duration of employment |
| Records relating to promotion, training, disciplinary matters | 5 years from reference / end of employment |

| | |
|---|---|
| References given / information to enable reference to be provided | 5 years from reference / end of employment |
| Summary of record of service (eg name, position(s) held, dates of employment) | 10 years from end of employment |

We will keep any client, volunteer or employee records as advised by legal representatives, where legal action has been started.

### VII. Appropriate security measures shall be taken against unauthorised or unlawful access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of or damage to personal data

Brighton Oasis Project Risk Management Policy includes an analysis of risk in relation to electronic and manual information records. See Section 11 for further information about Data Security.

Any security incidents will be logged, investigated and monitored.

### VIII. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data

Brighton Oasis Project will not transfer any subject data overseas, unless required to by law, or with the explicit consent of the subject (e.g. for overseas reference requests).

## 5. The Caldicott Guardian

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of service user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that the NHS, Councils with Social Services responsibilities (CSSRs) and partner organisations satisfy the highest practicable standards for handling patient identifiable information. Within BOP the Caldicott Guardian is the Director. The key responsibilities of the Caldicott Guardian are as follows:

**Strategy & Governance:** the Caldicott Guardian should champion confidentiality issues at Board/management team level, should sit on an organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

**Confidentiality & Data Protection expertise:** the Caldicott Guardian should develop a knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott function but also on external sources of advice and guidance where available.

**Internal Information Processing:** the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit.

**Information Sharing:** the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS and CSSRs. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related IT systems, disclosure to research interests and disclosure to the police.

## 6. Consent to Share Information Relating to Service Users

All information held on clients is confidential to Brighton Oasis Project and cannot be disclosed to third parties without the permission of the service user. The Confidentiality Waiver and the Carer's Confidentiality Waiver define the organisation's boundaries relating to information sharing and should be clearly explained to the service user. Their understanding of this and agreement should be logged by a signature on the appropriate form.

See the Confidentiality Policy for further information about this.

Any worker disclosing information to a third party without the service user's permission, except in exceptional circumstances (see below) will be subject to disciplinary procedures.

Each organisation should display posters and/or leaflets explaining:

1. Who the Data Controller is (e.g. the organisation who owns the data)
2. Why the information is needed
3. The purposes for which the information will be processed
4. Who will see the information (secretaries, administration staff)
5. The benefits to service users and to the organisation(s)
6. Any disclosures that may need to be made to other organisations (e.g. Acute Hospitals, Social Services, Meals on Wheels, Clinical Audit, GP Payments, Mental Health Teams, Drug Teams etc.)
7. The circumstances in which information may be passed on without consent (e.g., Child Protection, and Crime and Disorder)
8. Information restricted by legislation (e.g. HIV, Termination, etc.)
9. Information that must be passed on because of legislation (Births, Deaths, Cancer Registries etc.)

These posters and/or leaflets should be made available in other languages for those whose first language is not English or in a different form for those with a disability.

## 7. Disclosure of Information without Consent

Any child protection, criminal or substantial concerns about risk to a person's safety, can override any confidentiality agreement.

Decisions to disclose information about a service user to a third party without the service user's consent ideally should be discussed by at least that individual's key worker and the Services Care Co-Ordinator/ Director (the designated Caldicott Guardian), after an attempt has been made to persuade the service user to give consent. The final decision will be the Services Care Co-ordinator's/ Director's, or in their absence, the most senior worker's. The decision should be made without delay ensuring compliance with any local agreements for safeguarding vulnerable adults and children. The client will be informed of the Project's decision wherever possible.

In certain other circumstances, information may be shared without the permission of the individual concerned:

- Where there are concerns about the welfare of a child as defined by the Children Act 1989 (see Child Protection Policy)
- When required through a court order, or through a legitimate search warrant
- If a violent situation arises and the service user is endangering the safety of staff, other clients, or others
- Where there are suspicions that a serious crime has or may be committed, e.g. murder, sexual crime (as defined in the Sexual Offences Act 2003), terrorism (as defined in the Terrorism Act 2000), drug trafficking (as defined in the Drug Trafficking Act 1994)
    - Section 115 of the Crime and Disorder Act 1998 gives public bodies the power, *but not a duty,* to disclose information for the prevention or detection of crime
- When disclosures of physical or sexual abuse are made and others may still be at risk from the alleged perpetrator
- When allegations are made of a gross breach of trust or misconduct of a professional worker
- Circumstances where withholding information might result in serious harm to another
- To ensure the service provides a duty of care in a life-threatening situation (e.g. serious illness or injury, suicide and self-harming behaviour). This includes when a service user continues to drive against medical advice, when unfit to do so. In such circumstances relevant information should be disclosed to the medical advisor of the Driver and Vehicle Licensing Agency (DVLA) as soon as possible.

The responsibility for the final decision for divulging information to a third party without the client's permission lies with the Director (the Caldicott Guardian) or in her absence, the most senior worker

## 8. Requests for Information

Under the Data Protection Act 1998, service users have the right to access any person-identifiable information that is held about them at BOP. There is a process for this, including the receipt of a signed letter from the client, and a certain editorial process that may omit details made available to the service user under the grounds that it may cause serious harm to their (or others) mental or physical state, or that it contains information about a third party.

There are certain circumstances under which another party may request access to confidential information. If these parties are not covered by the Confidentiality Waiver, or legislation, then information may only be shared with proof of consent from the client. This could be faxed or posted to the organisation.

See Section 12 for information about requests for service user records from the police service.

The following guidance should be followed when sharing information with other agencies or workers:

"*Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely*." (Information Sharing: Guidance for Practitioners and Managers (2008) – see References)

## 9. Accessing Information without Consent

Employees may have the ability to access confidential information regarding individuals who are not service users, or information about service users that is not relevant to their work. It is an offence to access secure information without consent under The Computer Misuse Act 1990. Disciplinary action will be taken against staff members who have misused their privilege to access confidential information.

## 10. Information Sharing Security

No subject data will be given over the telephone unless the identity of the caller is verified. If the caller is unknown to the organisation, we will take a name and number and verify the caller's identity before disclosing service user information.

The fax machine, answerphone and telephones are sited or used in an area that is restricted to those who need to access the information.

If a fax contains confidential information, ensure someone is at the receiving end waiting for it.

Where possible do not use identifiable information in faxes – use a client number. NB – where there is a risk of harm to children or adults, this does not apply, as full information including names should be communicated as soon as is practicably possible in any risk scenario, for example, a child protection referral or a notification of a violent incident.

Employees are required not use identifiable information in emails, unless these can be encrypted.

Conversations which include confidential information should only take place within safe havens - ie behind closed doors.

Employees are required to ensure that they are sending the facsimile to the correct address and gain proof of receipt.

## 11. Recorded Data Security

All identifiable information held on service users must be kept secure – either in written/printed format in locked cabinets on premises, or in electronic format protected by passwords on a BOP computer or on the BOP virtual private network (VPN).

### 11.1. Written Records

Written records in which there is a client's name or enough information for a client to be identifiable to another party, should be kept in locked cabinets in areas where clients and the public do not have access at all times in which it is not in use. This includes at all times when the buildings are closed.

When not secured in cabinets, service user files or documents written about/by clients should not be left unattended in areas where non-staff members may be able to access them.

Files and records that contain person-identifiable information are disposed of either by shredding on site, or in the confidential waste bags which are subsequently sent to be shredded.

Service user files must not be removed from the premises.

### 11.2. Electronic Records

All electronically held confidential information must be protected by passwords, either on the VPN or on password protected computers provided by the organisation. Client information should not under any circumstances be stored on completed forms and templates on the VPN. It can be stored elsewhere where the author is satisfied that reference to them is required. These computers are equipped with the appropriate software to keep them as secure as is reasonably practicable (e.g. spyware scanners and firewalls) and the VPN password is regularly changed.

If computer hardware has ever been used to process personal data, it should only be disposed after reliable precautions have been taken to destroy any data stored.

All client information held on computer should be backed up every six weeks and back-up discs kept in lockable cabinets in areas where clients and the public do not have access unless accompanied by a staff member.

Any external contractors working on the Project's IT system or hardware, or working in the building, eg cleaners, must sign a confidentiality undertaking.

## 12. Information Sharing with the Police

BOP recognises the need for effective liaison with the police service in the interests of the safety of service users, staff and visitors. Any contact with the police in relation to service users should be recorded on their file.

There may be situations where there is contact with the police which can be sensitive or difficult and staff should be reminded to seek advice if required, or if in doubt, as to how best to proceed. Advice should be sought from either your line manager or the director.

Service user records may be made available to the Police under section 29 and 35 Part IV of the Data Protection Act 1998, to assist in the detection of crime or the apprehension or prosecution of offenders. However, in accordance with the Caldicott Committee Report (1997), the provision of such information should be assessed as "the need to know".

In all circumstances, no information from any records should be released until a Section 29 Disclosure request has been signed by a senior police officer, detailing what information is required and why, has been provided by the requesting police officer. A receipt should also be obtained, which is signed by the officer taking the information, which records their name, rank, force number and base. Under normal circumstances original documentation will not be released, photocopies only will be provided.

## 13. Third Party Reporting to the Police

The Brighton Oasis Project is signed up to a third party reporting protocol which places a duty on staff to report to the police incidents that they have knowledge of in which a person has come to harm. For more information on this see the Third Party Reporting Protocol.

# Responsibilities

### The Board / Management Committee

- Has overall responsibility for the policies and procedures at BOP, so far as is reasonably practical.

### The Director

- To ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Take the role of Caldicott Guardian for the organisation, championing the use of appropriate information sharing and a culture within the organisation which promotes and maintains confidentiality.
- To ensure that adequate resources and training is made available to staff on the subject of confidentiality.

### Line Managers/Care Co-ordinators

- To ensure that staff members are adequately informed about data protection and confidentiality procedures at induction and that this is maintained within the working culture at BOP.

### Staff Members & Volunteers

- To act with due care and attention for the confidentiality of the clients (both within and outside the workplace) and be aware of how and when confidentiality may be waived.
- To discuss any queries or concerns they may have about disclosures with a line manager or senior staff member.
- To ensure that the information they record or access is appropriately stored in secure cabinets or securely on computers.
- To ensure that they verify the authorisation of another person to ensure information is only passed on to those who have the right to see/hear it.
- Not to discuss confidential matters outside of work.
- To dispose of any confidential information in a secure manner (i.e. confidential shredding service, or emptied computer recycle bin).
- Not to access any confidential records/databases/files for personal reasons.
- To attend appropriate training as required.

## References

Information Sharing: Guidance for Practitioners and Managers (2008) - http://webarchive.nationalarchives.gov.uk/20130401151715/https://www.education.gov.uk/publications/standard/publicationdetail/page1/DCSF-00807-2008

Confidentiality: NHS Code of Practice (2003) - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

NTA – Confidentiality and Information Sharing (2003) – http://www.drugscope.org.uk/Resources/Drugscope/Documents/PDF/Good%20Practice/Confidentiality.pdf

NTA – Data Protection and Record Sharing (2003) –

http://www.dtmu.org.uk/sph-files/confidentiality/Data_Protection.pdf

NTA – Confidentiality Toolkit (2013) –

http://www.nta.nhs.uk/uploads/ndtmsconfidentialitytoolkitv6.3.pdf

NHS – Access to Records (2003) - http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_112916

NHS – Caldicott Guardians - http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

Caldicott Committee Report (1997) - http://www.hpa.org.uk/web/HPAweb&HPAwebStandard/HPAweb_C/1195733746440

FDAP Code of Practice (2008) - http://www.fdap.org.uk/code_of_practice.php

Children's Act 1989 – http://www.legislation.gov.uk/ukpga/1989/41/contents

Computer Misuse Act 1990 - http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm

Drug Trafficking Act 1994 - http://www.opsi.gov.uk/ACTS/acts1994/ukpga_19940037_en_1

Data Protection Act 1998 - http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

Human Rights Act 1998 –
http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

Crime and Disorder Act 1998 –
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980037_en_1

The Protection of Children Act 1999 –
http://www.opsi.gov.uk/ACTS/acts1999/ukpga_19990014_en_1

Terrorism Act 2006 –
http://www.legislation.gov.uk/ukpga/2006/11/contents

Freedom of Information Act 2000 -
http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

Health & Social Care Act 2001 –
http://www.opsi.gov.uk/Acts/acts2001/ukpga_20010015_en_1

Sexual Offences Act 2003 –
http://www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1

# Appendix A – The Data Protection Act 1998

## THE EIGHT PRINCIPLES

For personal data held in any format

**1.** The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

**2.** Personal data shall be obtained only for one or more specified lawful purpose(s). Personal data held for any purpose or purposes shall not be further used or disclosed in any manner incompatible with that purpose or purposes.

**3.** Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or purposes.

**4.** Personal data shall be accurate and, where necessary kept up to date.

**5.** Personal data held for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

**6.** Personal data shall be processed in accordance with the rights of the individual under this Act. An individual shall be entitled:

- At reasonable intervals and without undue delay or expense:
    - To be informed by any data user whether he or she holds personal data of which the individual is the subject, and
    - To access any such data held by the data user, and
- Where appropriate to have such data corrected or erased

**7.** Appropriate security measures shall be taken against unauthorised or unlawful access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of or damage to personal data.

**8.** Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

# Appendix B – FDAP Code of Practice for Drug and Alcohol Professionals

Drug and alcohol practitioners provide a wide range of substance misuse related services including: education and prevention; services to people with drug and alcohol problems; services to those affected by drug and alcohol use; and professional services to other practitioners. This Code of Practice covers all such activities.

## 14. General

1. Drug and alcohol practitioners seek to help reduce the damage caused by substance misuse to users themselves, those close to them and the wider community, and this goal should guide their work at all times.
2. Drug and alcohol practitioners should act in a professional and responsible way at all times. They should be honest and fair in their professional dealings, act with integrity, be conscientious, careful and thorough in their work, and take account of their obligations under the law and to the wider public interest.
3. Practitioners must at all times respect the rights, dignity and interests of their clients. They should treat all clients equitably, and must not discriminate on grounds of lifestyle, gender, age, disability, race, sexuality, religion, beliefs, culture, ethnicity, or financial or social status against clients, colleagues, or anyone else with whom they have dealings in the course of their work.
4. In making statements to clients, other professionals and the general public, practitioners should recognise the difference between fact and opinion, acknowledge where professional opinions differ, and state as fact only what has been empirically validated as such.
5. Practitioners should ensure that their work is adequately covered by insurance for professional indemnity and liability, whether through their employer or independently.

## 15. Service provision

1. Any service provided by a practitioner should be based on an assessment of the individual's need, and take account of the practitioner's professional responsibilities and the relevant evidence base on effective practice.
2. Treatment services should be based on a treatment plan, drawn up in consultation with the client concerned.
3. Practitioners should provide a service only where they feel that it would, taking account of their professional responsibilities, be appropriate for them to do so, and should ensure that those concerned are aware of any alternative options open to them.

4. Practitioners who receive payment or other benefits from service providers for advising people about, or referring them to, their services must make this clear to all concerned and not allow their own financial interests to compromise their wider professional responsibilities.
5. Where a practitioner feels it would be inappropriate for them to provide a service they should take all reasonable steps to help find a suitable alternative where appropriate.

## 16. Professional competence

1. Practitioners should keep their knowledge and skills up-to-date. They should not attempt to work beyond their competence.
2. Practitioners should take care to present their qualifications and experience accurately and to avoid them being misrepresented.
3. Practitioners should refrain from practice when their ability to act professionally is impaired as a result of a psychological or physical condition, *eg* an on-going or recent alcohol or drug related problem, illness, personal stress *etc*. Where a practitioner is under any doubt on this they should seek the guidance of their supervisor and should notify their supervisor & employer of any recent or on-going drug or alcohol problem.
4. Except for medication taken under direction of a doctor, practitioners should not take any mood altering substance, including alcohol, prior to, or while carrying out, their work. Practitioners should never practice while their competence is impaired by the use of any mood altering substance.

## 17. Consent

1. Before providing a service, practitioners should secure the informed consent of the person concerned (or their legal representatives) - and must take all reasonable steps to ensure that the nature of the service, and anticipated consequences, are adequately understood.
2. Written consent must always be secured for a person's involvement in research - and information about the purpose or nature of a research study should be withheld only where this is approved by an appropriately constituted ethical committee made up of other practitioners and lay representatives.
3. Practitioners must recognise that in some situations a person's capacity to give valid consent may be diminished and should take this in to account before agreeing to provide a service, Practitioners must never use any form of coercion to obtain consent.
4. Practitioners must not make false or exaggerated claims about the effectiveness of the services they are providing, nor should they ascribe unusual powers to themselves.
5. If conditions are imposed upon the continuation of a service, they must have the approval of a senior colleague or supervisor and be considered to be clearly consistent with the practitioner's professional responsibilities. Such conditions must always be clearly explained to the client.

6. Practitioners must recognise and uphold a client's right to withdraw consent at any time.

## 18. Confidentiality

1. Personally identifiable information about clients should normally be disclosed to others only with the valid informed consent of the person concerned (or their legal representatives) - and the boundaries and limits of confidentiality should be explained clearly before any service is provided.
2. Where a practitioner holds a sincere belief that a client poses a serious risk of harm to themselves or others, or where obliged by law, a practitioner may be required to disclose personally identifiable information without the client's consent. Before breaking confidentiality, however, practitioners should still seek to secure valid consent for disclosure from the person concerned and should consult with their supervisor or a senior colleague where this is not provided - except where the practitioner judges that any delay this might cause would present a significant risk to life or health, or place the practitioner in contravention of the law.
3. Information identifying clients must never be published (for example in an article or book), without their written agreement (or that of their legal representatives).
4. All reasonable steps should be taken to ensure that any records relating to clients are kept secure from unauthorised access and the requirements of the Data Protection Act should be complied with at all times.

## 19. Client relations

1. Practitioners must recognise that they hold positions of responsibility and that their clients and those seeking their help will often be in a position of vulnerability.
2. Practitioners must not abuse their client’s trust in order to gain sexual, emotional, financial or any other kind of personal advantage. Practitioners should not engage in sexual relations, or any other type of sexualised behaviour, with or towards clients.
3. Practitioners should exercise considerable caution and consult their supervisor before entering into personal or business relationships with former clients and should expect to be held professionally accountable if the relationship becomes detrimental to the client or to the standing of the profession.
4. Practitioners should not carry out an assessment or intervention with, or provide supervision to, someone with whom they have an existing relationship. In the event of a practitioner having an existing relationship with any person who is referred to an agency in which they work, this should be drawn to the attention of the practitioner's line manager and supervisor.
5. It is recognised that some practitioners are involved in on-going self-help / peer support groups, and that they may on occasions come in to contact

with existing or former clients within this context. Any such contact must be handled carefully. If a practitioner is asked by a former client to act as a 'sponsor' in such a context, the practitioner should seek guidance from their supervisor before agreeing to do so.

## 20. Professional supervision

1. All practitioners should have regular professional supervision, focusing on reviewing, guiding and supporting their practice. If such supervision is not provided by an employer it should be obtained elsewhere.
2. Where a practitioner has any serious doubts about how to handle a particular situation, including in relation to this code of practice, they should discuss this with their supervisor / line manager at the earliest opportunity.

## 21. Professional standards

1. Practitioners must disclose to their employer and supervisor any past disciplinary action taken against them by an employer or professional body in relation to unprofessional or unethical conduct.
2. Practitioners must not condone, support, conceal or otherwise enable the unethical conduct of colleagues. Where they are aware of, or have good reason to suspect, misconduct on the part of a colleague this should be discussed with the practitioner's own line manager or supervisor and under their guidance should be drawn to the attention of the colleague's line manager, supervisor and/or professional body - taking account of the need to respect clients' rights of confidentiality.
3. Practitioners have a duty to explain to clients their rights and options in making a formal complaint about a service they have received, whether the service was provided by the practitioner him/herself or by a fellow practitioner. Practitioners must never attempt to prevent or dissuade a client from making a complaint about a service with which they are dissatisfied.