Service User Confidentiality Policy

Dun Laoghaire Rathdown Outreach Project

Approval date: January 2016

Next Revision date: January 2018

1.Responsibility for approval of policy	Governance and Human Resources Subcommittee
2.Responsibility for implementation	Manager
3.Responsibility for ensuring review	Manager

1. Policy Statement

Confidentiality is a central and integral part of the Dun Laoghaire Rathdown Outreach Project (DROP). DROP is committed to ensuring that all service user information is managed in line with accepted good practice and relevant legislation.

2. Purpose

2.1. To ensure that the confidentiality of people using the services of the organisation is protected in a consistent and appropriate manner.

2.2. To provide staff, sessional workers, students, volunteers and service users with the organisation's understanding of confidentiality; clear guidelines regarding handling of information, including the sharing of information and the extension of confidentiality

2.3. To assign responsibilities for the management of confidentiality.

3. Scope

3.1. This policy covers all DROP staff, sessional workers, students and volunteers. This policy also applies to persons from other services conducting in-reach.

3.2. This policy applies to service users over 18 years of age.

4. Legislation and relevant documents

4.1 Children First, National Guidance for the Protection & Welfare of Children (2011)

4.2 Children's Act 2001

4.3 Child Care Act 1991

4.4 Data Protection Act 1988

4.5 Data Protection (Amendment) Act 2003

4.6 Consent to Share Information Form Appendix 1

4.7 National Protocols and Common Assessment Guidelines to Accompany the National Drugs Rehabilitation Framework

4.8 DROP's Data Protection Policy

5. Glossary of Terms and Definitions

5.1. Confidentiality

All information that is obtained through the course of organisational business and service provision is confidential, and staff, sessional workers, students or volunteers shall not at any time, whether before or after the end of their involvement, disclose such information in any form to any person without written consent. Exceptions to this are outlined in – point 10: Limits to confidentiality.

5.2. Sharing without consent

In certain circumstances information can be passed on to a third party without the consent of the individual whose information it is. These circumstances are described in legislation and relate to the safety of the individual or others. Outlined in point 10.

5.3 Wrongful Disclosure

Is disclosure without consent, whether accidental or deliberate, which is not covered by section 10.

6. General

6.1. Confidentiality can never be absolute and therefore absolute confidence can never be guaranteed.

6.2. All service users are to be made aware of DROP's confidentiality policy. Service users will have access to this confidentiality policy.

6.3. All service users have the right to have a copy of any information held regarding them by DROP. This must be requested in writing by the services user, and will be dealt with by the Manager; all requests will be responded to within 21 working days.

6.4. Confidentiality is between the service user and the organisation. It is not between the service user and any particular member of staff. Case specific information will be shared with the staff team where relevant and necessary.
6.5. No information about a service user will be passed on to any third party except in the following cases:
  6.5.1. Where consent has been obtained.
  6.5.2. Where there is a legal obligation to extend confidentiality ie share information.
  6.5.3. Where a decision is taken by management to share information as per the terms of this policy.
6.6. All service users have the right to withdraw consent for the sharing of information at any time, except where there is a legal obligation for confidentiality to be extended; as outlined in section 10.
6.7. All service user files are to be kept in a secure place within the organisation. Staff, sessional workers, students and volunteers are expected to exercise care to keeping safe all documentation or other material containing confidential information.
6.8. All service users' files should be kept in a locked filing cabinet, with the key held only by staff members involved in relevant service provision.
6.9. Computer files should be password protected with the password held only by staff members involved in relevant service provision.

7. Roles and Responsibilities

Dun Laoghaire Rathdown Outreach Project is responsible for ensuring that all staff, sessional workers, students and volunteers involved in dealing with confidential information and data receive appropriate training, supervision and support regarding the policy and their legal responsibilities.

7.1. Responsibility:
The manager is responsible for ensuring that a copy of this document is available to all staff, sessional workers, students and volunteers and is available to users of the service. It is the responsibility of the manager to ensure that all staff sign to confirm they have understood the confidentiality policy and that they receive training as necessary.
7.2. Individual's Responsibility:
All staff, sessional workers, students and volunteers are required to act in accordance with the policy, failure to do so will be considered as an act of gross misconduct and will result in disciplinary action.

8. Informing Service Users

8.1. All service users should be made aware of the following:
  8.1.1. Confidentiality is between the individual and the organisation; information will be shared with the staff team.
  8.1.2. Their right to have a copy of all information concerning them and that they will need to request this in writing, which staff can support them to do.
  8.1.3. Circumstances in which confidentiality may be extended, see point 10.
  8.1.4. Their consent to share information can be withdrawn at any time.
8.2. This information should be imparted at the point of initial contact / assessment and at regular intervals while accessing our services by the staff member undertaking this work.

9. Obtaining Consent to Share Information

9.1. Information held by the organisation, and not independently available to a third party, cannot be disclosed without the individual's written consent.
9.2. Consent must be sought in writing using a standardised consent form. The service user should be informed each time information regarding them will be shared with a third party.
9.3. The consent form should stipulate:
  9.3.1. The third party with whom the information is to be shared.

9.3.2. The period time for which consent is given. Written consent to share information cannot be given for periods longer than six months. Once the initial period for which the written consent is valid has expired, fresh written consent must be sought.
9.3.3. The specific details concerning the information that will be shared including what information can be shared and through what mode of communication (i.e. in person, fax, telephone, email, in writing).
9.3.4. The date and signatures of the service user and DROP

9.4. Each time it is sought to share information under the written consent, the service user should verbally be informed of:
9.4.1. The third party with whom the information is to be shared
9.4.2. Whether the third party has a confidentiality policy
9.4.3. The reason for sharing the information
9.4.4. That DROP has no control over the information once it is given to a third party.
9.4.5. That they can withdraw their consent to share information if they so wish

10. Limits to Confidentiality

10.1. Confidentiality can never be absolute and therefore absolute confidentiality can never be guaranteed. Limits to confidentiality exist to protect workers from withholding information that may require immediate action in the interest of public or individual safety.
10.2. Application of extensions of confidentiality will in all cases be decided by the Manager, in their absence this decision will be delegated to the most senior staff person.
10.3. Confidential information may be shared with an external third party without service user consent when:
10.3.1. They have perpetrated sexual / physical abuse on another person
10.3.2. They intend to perpetrate sexual / physical abuse on another person
10.3.3. Any other issues in relation to Child Protection, as described in Children First
10.3.4. They have committed a criminal act (Criminal Law Act, 1997)
10.3.5. They intend to commit a criminal act (Criminal Law Act, 1997)
10.3.6. They have self-harmed / attempted suicide and are at risk of causing harm to self
10.3.7. They intend to self-harm / attempt suicide
10.4. In the event of a disclosure of any of the above, the staff member should inform the service user that they will need to report the issue to their Line Manager. If it is necessary to pass on the information the service users consent should be obtained if possible, if not possible at the time the service user should be informed at the next available opportunity.
10.5. Other situations where consent may be extended:
10.5.1. As required by law, including though not limited to court appearances.

11. Sharing Information with Other Organisations

11.1. In all cases, there must be a written consent form, signed by the service user, on file before any information is to be shared with any third party. In the event that the consent form does not originate from DROP the validity of the consent form received must be confirmed verbally with the service user before any information is shared.
11.2. If DROP is requested to write a service report, where possible this will be shown to the service user for comment prior to it being sent.
11.3. Care must be taken in relation to specific modes of communication to ensure confidential information is not unintentionally shared. Always ensure that consent covers the type of communication by which it is intended to share information.
11.3.1 Emails should be sent to organisational, not personal email addresses. Be aware that emails are not a secure method of communication unless encrypted. DROP does not operate an encrypted email system to external domains. Thus, if email is to be used as a method of communication, the

service user whose information is to be shared must specifically agree to transmission by this method and be advised of the risks of same which include;

11.3.1.1 The email may be intercepted in transit

11.3.1.2 The email may be forwarded or otherwise dealt with by the recipient

11.3.2 Phone calls do not allow us to see who we are talking to. There is risk that the person calling is not who they say they are. Service user attendance or presence in the service must not be confirmed to a caller unless you are sure they are covered by a valid consent form.

11.3.3 Fax number should be confirmed as organisational numbers. It is also useful to confirm where in the building a fax machine is located to ensure that faxed confidential information does not arrive in a public place.

11.4. Staff members called to give evidence in court should contact the Manager, who will provide support in this area.

11.5. All requests for service user involvement in research, evaluation or for other data collection purposes need to have ethical approval from a recognised body and must include clear guidelines on confidentiality. All such requests must be approved by the Manager prior to these being facilitated by staff or displayed within the organisation. Any such research should comply with data protection guidance on research.

12. Wrongful Disclosure

12.1. Wrongful disclosure will be considered as an act of misconduct or gross misconduct as appropriate and may result in disciplinary action.

12.2. Where wrongful disclosure has taken place, the service user will be informed.

12.3. DROP will inform the office of the data commissioner of the wrongful disclosure, as appropriate.

13. Data Protection Responsibilities

13.1. In addition to the duty of care regarding confidentiality outlined above, the Data Protection Acts imposes legal obligations on DROP, its staff and volunteers. DROP takes seriously its responsibilities under the Data Protection Acts. The organisation is aware of and acts in accordance with the following eight Data Protection principles regarding information:

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose information only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure it is adequate, relevant and not excessive
7. Retain for no longer than is necessary
8. Allow individual's access to their personal data, on request

13.2. DROP's Data Protection Policy outlines our data protection practices and procedures and is available on the shared network.

14. Service User Request for Information

14.1. If a service user wishes to have access to their file, they need to complete a written request; staff can assist with this.

14.2. The request will be processed by the/ Manager who will process the request within 21working days.

14.3. In this case care will be taken to ensure that any information relating to other individuals that is held within the service users file is blanked out.

Appendix 1 – Consent to share Information form

DUN LAOGHAIRE RATHDOWN OUTREACH PROJECT CLG
CONSENT TO SHARE INFORMATION FORM

Date: _____

Service User name: _____

Address: _____

_____

I give permission to DROP to share information regarding me with:

Name	Position	Service / Agency

This communication can take place:
Please tick as appropriate.

In person □
By telephone □
In writing □
By email □
By fax □

This communication can include issues relating to:
Please tick as appropriate.

Accommodation	□	Income and Finance	□
Family	□	Physical health	□
Childhood	□	Mental health	□
Education	□	Alcohol use	□
Work/Training	□	Drug use	□
Legal Issues	□	Independent living skills	□

I would / would not like to see any letters / emails concerning me before they are sent to the person(s) or organisation(s) mentioned above. I confirm that I understand the Dun Laoghaire Rathdown Outreach Project's confidentiality policy, and the times when information may be shared without my permission.

Signed (Service User) _____

Signed (Staff member) _____

Review date _____

CONSENT TO RETAIN MY PERSONAL INFORMATION

I confirm that it has been explained to me that a client file with my personal information will be kept in the Dun Laoghaire Rathdown Outreach Project.

This information will be a record of my participation in the service that DROP provides me and any correspondence provided to me and on my behalf from the organisation. The information will be retained in a secure manner and in both written and electronic format.

I confirm that I have been informed that I can access the organisation's Data Protection policy at www.drop.ie and should I wish to access my file can do so following the procedures outlined in this policy ☐ (please tick)

Signed (Service User) _____

Signed (Staff member) _____

Date: _____