

---

# Service User Confidentiality Policy

---

Turas Training

---

Approval date: July 2017

---

Revision date: March 2019

---

## 1. Policy Statement

- 1.1 The confidentiality of service user information is a central and integral part of TURAS'S service delivery. TURAS 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, volunteers and service users with the organisation's understanding of confidentiality and clear guidelines regarding handling of information, including the extension of confidentiality.
- 2.3. To assign responsibilities for the management of confidential information.
- 2.4. **Please see appendix 2 for conditions of use.**

## 3. Scope

- 3.1. This policy covers all TURAS employees, locums and volunteers.
- 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 and Welfare of Children (2011)
- 4.2. The Children Act 2001
- 4.3. Child Care Act 1991
- 4.4. The Data Protection Act 1988
- 4.5. The Data Protection (Amendment) Act 2003
- 4.6. The Freedom of Information Act 1997
- 4.7. The Freedom of Information (Amendment) Act 2003
- 4.8. Consent to share form (appendix 1)
- 4.9. National Protocols and Common Assessment Guidelines to accompany the National Drugs Rehabilitation Framework
- 4.10. TURAS Data Protection policy

## 5. Glossary of Terms and Definitions

- 5.1. Personnel: in this document, personnel are used as a collective term to cover all persons to whom this policy applies.
- 5.2. Service user: in this document, a 'service user' is someone who utilises Turas's services.
- 5.3. Confidentiality: All information that is obtained about a service user through the course of organisational business and service provision is to be treated as confidential to the organisation. Personnel shall not at any time, whether during or after their involvement with Turas disclose such information in any form to a third party without the prior written consent of that service user. Exceptions to this are outlined in section 10: Limits to confidentiality.
- 5.4. Sharing without consent: In certain circumstances information about an individual service user may be passed on to a third party without the consent of that service user. These circumstances are outlined in section 10: Limits to confidentiality.
- 5.5. Wrongful disclosure: Is disclosure without consent, whether accidental or deliberate, which is not covered by section 10.

## 6. Roles and Responsibilities

- 6.1. The project coordinator is responsible for:
  - 6.1.1. Ensuring that a copy of this document is available to all personnel including service users.
  - 6.1.2. Ensuring that all relevant personnel receive training as necessary and sign to confirm they have understood read, understood and agree to be bound by the confidentiality policy.

- 6.2. All personnel are responsible for working in accordance with this policy. Failure to do so will be considered as an act of misconduct or gross misconduct, as appropriate, and may result in disciplinary action.

## 7. General Guidelines

- 7.1. Confidentiality can never be absolute and therefore absolute confidentiality can never be guaranteed.
- 7.2. All service users are to be made aware of Turas's confidentiality policy as soon as is practicable after they first access Turas's services
- 7.3. All personnel and service users will have access to this confidentiality policy.
- 7.4. Confidentiality is between the service user and Turas It is not between the service user and any particular member of staff. Case specific information will be shared with the organisational personnel as relevant and necessary.
- 7.5. Confidential information should only be shared with, or accessible to, personnel covered by this policy where needed for the proper care of the person to whom it relates
- 7.6. All service users have the right to have a copy of any information held regarding them by Turas with the proviso that, where certain information in the file identifies other people to whom the organisation owes a duty of confidentiality, such information will be redacted. Copy information must be requested in writing by the service user. Staff members should assist with this as appropriate. The project coordinator will deal with all such requests; the organisation endeavours that all requests will receive a response within ten working days.
- 7.6 No information about a service user will be passed on to any third party except in the following cases:
- 7.6.1 Where consent has been obtained under this policy
- 7.6.2 Where there is a legal obligation to provide information to a third party
- 7.6.3 Where a decision is taken by management to share information with a third party as outlined in section 10.
- 7.7 Consent to share information with a third party should always be given initially in writing, and thereafter may be given verbally. Service users have the right to withdraw consent for the sharing of information at any time, except where the organisation decides, or is obliged, to share information, as outlined in section 10.
- 7.8 All service user files are to be kept in a secure place within the organisation. Personnel are expected to exercise care to keeping safe all documentation or other material containing confidential information in line with the organisation's Data Protection policy.
- 7.8.1 Paper files should be kept in a locked filing cabinet, with the key held only by personnel involved in relevant service provision.
- 7.8.2 Computer files should be password protected with the password held only by personnel involved in relevant service provision.

## 8. Informing Service Users

- 8.1. All service users should be made aware of the following at the first point of contact with Turas
- 8.1.1 That they have a right to confidentiality of their personal information
- 8.1.2 That confidentiality is between the individual and [NAME OF ORGANISATION]; information will be shared with the staff team.
- 8.1.3 That they have a right to have a copy of all information held by the organisation concerning them, and that if they want a copy of same, they will need to request this in writing, which staff can support them to do.
- 8.1.4 That confidentiality is not absolute, and the circumstances in which information about them may be shared with a third party, as set out section 10.
- 8.1.5 That their consent to share information can be withdrawn by them at any time, except where circumstances in which information about them may be shared with a third party, as set out section 10, apply

## 9. Obtaining Consent to Share Information

- 9.1. Information held by the organisation about a service user, and not independently available to a third party, cannot be disclosed without that service user's prior written consent.
- 9.2. Consent must be sought initially in writing, using a consent form. Thereafter it should be sought verbally. The service user should be informed each time information regarding them will be shared with a third party.
- 9.3. Written consent to share information cannot be given for periods longer than 6 months. Once the initial period for which the written consent is valid is expired, fresh written consent must be sought.
- 9.4. The consent form should stipulate:
  - 9.4.1 The third party(s) with whom the information is to be shared
  - 9.4.2 The period of time for which consent is given
  - 9.4.3 Specific details concerning the information that will be shared including what information can be shared and through what mode of communication (e.g.: in person, fax, telephone, email, in writing)
  - 9.4.4 The date and signatures of the service user and their keyworker
- 9.5 Each time it is sought to share information under the written consent, the service user should verbally be informed of:
  - 9.5.1 The third party with whom the information is to be shared
  - 9.5.2 Whether the third party has a confidentiality policy
  - 9.5.3 The reason for sharing the information
  - 9.5.4 That TURAS has no control over the information once it is given to a third party.
  - 9.5.5 That they can withdraw their consent to share 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 personnel from withholding information that may require immediate action in the interest of public or individual safety.
- 10.2. Decisions to share confidential information where no valid consent exists will, in all cases, be decided by the management team. In the absence of the application of a factor under 10.3, information will only be shared where it is in the interests of the person to whom the information relates to do so.
- 10.3. Confidential information may be shared with an external third party without service user consent when:
  - 10.3.1 The service user discloses information which reveals a substantial risk of harm to self or others.
  - 10.3.2 There is a suspicion or risk of harm to children. The service will, in this instance, follow the guidelines and reporting procedure as set out in *Children First: National Guidance for the Protection and Welfare of Children* (Dept. of Children and Youth Affairs, 2011).
  - 10.3.3 There is a court or tribunal order, or as otherwise required by law.
  - 10.3.4 In other circumstances as set out by Section 8 of the Data Protection Act, 1988
- 10.4. If a service user discloses information which may require to be shared, the staff member should inform the service user that they will report the issue to their line manager. If it is decided that the information will be shared, the service user's consent should be obtained if possible. If this is not possible, the service user should still be informed of the decision to share the information, if possible.

## 11. Sharing Information with External Third Parties

- 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 other external third party. In the event that the consent form does not originate from Turas the validity of the consent form received must be confirmed verbally with the service user before any information is shared.
- 11.2. If TURAS 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 incorrectly 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. Turas 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 be 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 a 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 we are sure they are covered by a valid consent form.
  - 11.3.3. Fax numbers 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. If a staff member becomes aware of information relating to a service user from sources outside Turas and where no consent to share information is in place, this information should be taken to their line manager in the first instance who will make a decision as to whether, in all the circumstances, further action needs to be taken. Further action could include, but is not limited to:
  - 11.4.1. Telling the service user about the information
  - 11.4.2. If the information comes from another organisation, making a formal complaint to that organisation
  - 11.4.3. Other action as the information warrants
- 11.5. Staff members called to give evidence in court should contact the management who will provide support in this area.
- 11.6. 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. Any such research should comply with Data Protection guidance on research, a copy of which is available at [www.turastraining.ie](http://www.turastraining.ie). All such requests must be approved by the management team prior to these being facilitated by staff or displayed within the organisation.

## 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. TURAS 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 Turas its staff and volunteers. Turas takes seriously its responsibilities under the Data Protection Acts. The organisation is aware of and acts in accordance with the following eight Data Protection rules<sup>1</sup> regarding information:
  - 13.1.1. Obtain and process the information fairly
  - 13.1.2. Keep it only for one or more specified and lawful purposes
  - 13.1.3. Process it only in ways compatible with the purposes for which it was given to you initially
  - 13.1.4. Keep it safe and secure
  - 13.1.5. Keep it accurate and up-to-date
  - 13.1.6. Ensure that it is adequate, relevant and not excessive
  - 13.1.7. Retain it no longer than is necessary for the specified purpose or purposes
  - 13.1.8. Give a copy of his/her personal data to any individual, on request.

---

<sup>1</sup> See <http://www.dataprotection.ie>

- 13.2. Turas Data Protection Policy outlines our data protection practices and procedures and is available at [www.turastraining.ie](http://www.turastraining.ie).

#### **14. Service User Request for Information**

- 14.1. If a service user wishes to have a copy of the information the service holds on them, they should complete a written request; staff can assist with this.
- 14.2. The request will be processed by the line manager who will process the request within ten working days.
- 14.3. In this case care will be taken to ensure that any information naming, or which could be used to identify, other individuals that is held within the service user's file is blanked out.

## Consent to Share Information Form

Date: \_\_\_\_\_

Client name: \_\_\_\_\_

Address: \_\_\_\_\_

\_\_\_\_\_

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

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

### 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

Family

Childhood

Education

Work/Training

Legal Issues

Other, Please specify

Income and Finance

Physical health

Mental health

Alcohol use

Drug use

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 [INSERT ORGANISATION]'s confidentiality policy, and the times when information may be shared without my permission.

Signed (Client) \_\_\_\_\_

Signed (Staff member) \_\_\_\_\_

Duration of Consent From \_\_\_\_\_ To \_\_\_\_\_

Review date \_\_\_\_\_

## Appendix 1 - Conditions of Use

1. I understand that this document is a draft policy template. This draft policy template must not be implemented without being amended by individual organisations, following a consultation process with relevant stakeholders.
2. I understand that while significant effort has been put into the production of this draft policy template, no claim is made as to its accuracy or veracity by Ana Liffey Drug Project, its members and/or agents, including expert reviewers.
3. I understand that use of this draft policy template is entirely at the risk of the person/organisation accessing it. Ana Liffey Drug Project, its members and/or agents, including expert reviewers exclude all liability for any loss or damage arising from implementation or use of this draft policy template, howsoever caused.
4. I understand that this draft policy template remains the copyright of the Ana Liffey Drug Project. I undertake not to sell on or otherwise profit from this draft policy template. I acknowledge that "Ana Liffey Drug Project" must be noted as a source if this draft policy template is used for reasons other than in relation to Quality in Alcohol and Drug Services.

By downloading and using this draft policy template, I indicate that I have read, understood and agree to be bound by the conditions of use.