2.2 Confidentiality Policy 2016

ESSENTIAL DRUG & ALCOHOL SERVICES

CONFIDENTIALITY POLICY & PROCEDURE

Date of Adoption: Board Meeting 5 -2016 Signed: L Clarke. (EDAS Chair)

Date of next review: Board Meeting 5 2019 By Whom: EDAS Board of Trustees

To be read in conjunction with the following:

Safeguarding Children Policy
Safeguarding Vulnerable Adult Policy
Whistleblowing Policy
Complaints and Compliments Policy
Grievance Procedure
Disciplinary Policy
Equal Opportunities Dignity & Diversity Policy

Policy

At the heart of EDAS's confidentiality policy is our commitment to treat people who use our services, staff and other stakeholders with the utmost respect and in a manner which will always aim to preserve their dignity. EDAS recognises that unauthorised disclosure of information may put an individual at risk of harm.

EDAS will not routinely disclose information about people who use its services, or about staff and the internal business of the organisation to anyone.

Confidential information can be any information that relates to services users, staff, their family and friends, however stored.

When referring people who use our services to other agencies, EDAS will only disclose information, having asked permission directly from the person involved and having their informed consent to do so. This confidentiality rule applies both to individuals and to workers from other agencies approaching EDAS for advice, information or support.

EDAS recognises that there are instances where a better service can be provided by sharing information about a service user with other relevant agencies. This could be to prevent duplication, ensure coordination of services or to protect a child or vulnerable adult. EDAS workers should only share such information on a 'need to know' basis and should seek the consent of and inform the service user they are doing this. It is only in exceptional cases (documented below) that a worker should share information about a service user without informing them and gaining their consent.

This policy applies to all staff. In the context of this policy the term 'staff' is defined as all salaried staff, volunteers, students on placements, trustees and any other individuals accountable to EDAS.

2.2 Confidentiality Policy 2016

All people working with EDAS, whether as paid employees or in a voluntary capacity, are required to sign a Confidentiality Contract to the Service (See Appendix 1). Anyone working for EDAS who breaches these Contracts will be liable to Disciplinary Procedures, which could be classed as gross misconduct and result in dismissal.

This Policy aims to provide:

- Guidance for all staff to follow to protect themselves so that they do not inadvertently breach any of the expectations required of them by law. The Data Protection Act should not be a barrier to sharing information, but provide guidelines about when to share.
- To understand what information is confidential and how staff can work to keep it confidential
- To clearly show when information should be shared.

Responsibilities

All staff are responsible for the strict compliance with the Confidentiality Policy and should ensure that their practices reflect EDAS's guidance on confidentiality.

With regard to service delivery, Team Leaders and Line Managers will monitor staff practice and discuss any issues relating to confidentiality at supervision and team/clinical meetings. They will discuss with the CEO decisions in situations where it is not clear as to whether or not information should be shared without the consent of the person to whom the information relates to; this will be documented for auditable purposes (e.g. in client notes/supervision records).

Guidelines for Information Sharing

The Seven golden rules are:

- The Data Protection Act is not a barrier to sharing information but provides a framework
- Be Open and Honest
- Seek advice from your Line Manager/Clinical Lead
- Share with consent where appropriate
- Consider safety and well-being
- Share only necessary, proportionate, relevant, accurate, timely and secure Information
- Keep a Record

Working Guidelines

Staff will NOT:

- Talk about service users in public places or where they may be overheard
- Leave any confidential or private information unattended.
- Look at any information relating to their own family, friends or any individual unless they are directly involved in an individual's care and recovery
- Talk about users of services if it is not related to the specifics of their role. i.e. No gossiping
- Divulge Passwords, or write them down

- Divulge personal information relating to other staff (without their consent) which they have come to know in the course of their work, unless there is a clear, work-related reason for them to do so. Where staff are concerned about the welfare of other staff or have information which they believe is impacting upon a member of staff's ability to carry out their duties, they should inform their Line Manager or Clinical Lead/CEO. Concern for another member of staff's welfare is not a valid reason to divulge personal information (without consent) about that person to their colleagues.
- Divulge personal information relating to other staff, service users or EDAS business (without consent) to staff who previously worked for EDAS; in particular those who were privy to confidential information
- Talk to the media – Only the Chief Executive is permitted to provide information to the media.

Practice:

At any initial meeting with people who use EDAS's services, the worker will explain responsibilities regarding confidentiality to the individual. They will explain how information will be kept confidential and when and what they would need to share. If at any point it seems appropriate to repeat this to the individual to help them and reaffirm working practice then it should be repeated.

All individuals must be informed that information is confidential to the Service, and not to the individual worker, and why that is so.

If workers are in doubt over any instance, they should always consult with their line manager.

If the friend or relative of a person using the service is also using EDAS services, information should not be given from one friend/relative to another, again without specific permission.

The right to withhold or withdraw consent

Service users have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might be able to provide essential services. They can also withdraw consent given at any time.

Where individuals are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. Service users will be asked to sign and date a new confidentiality form to confirm the changes in consent.

Requests for Information

Workers should not give information about a user of EDAS's services or member of staff to anyone outside the organisation, either voluntarily or on request, unless the person concerned has specifically given their permission, preferably in writing (permission given at assessment can constitute permission in writing). Where possible, workers should verify the identity of the person making the request and should say they cannot confirm or deny that the person is accessing the service unless the service user has given consent to share the information with the individual.

Workers should be able to clearly and respectfully explain to people the reasons why they cannot share information. Where the person making the request is struggling to understand the policy, they should be referred to the worker's Line Manager.

Multi-agency Working

As EDAS works in close collaboration with a number of other agencies, the boundaries of confidentiality with each worker must be clear and information sharing protocols must be adhered to.

Where three-way work is undertaken with a client, worker and professional from another agency, the bounds of confidentiality between all three should be negotiated and documented at the outset, with copies to all three parties. This may constitute Informed Consent, and thereby enable all parties to share relevant information routinely.

Where the service user is satisfied it is in their own interest for information to be divulged to EDAS by other professionals, workers should ask to see a signed consent form from the service user. If time is of the essence, verbal assurance that the service user has given their Informed Consent will suffice with professionals with whom we have a standing working relationship, particularly if we can gain written consent retrospectively. Any verbal assurance needs to be documented in case notes. EDAS accepts faxed copies of consent forms.

At assessment and at care plan reviews (held at least every 6 months), it is routine to ask the service user which other agencies and professionals they are already in contact with. They are then asked if we have permission to discuss relevant matters with them, to facilitate sharing of information, this is then clearly document in case notes and the signing of a new confidentiality/information sharing consent form is requested.

Information storage/use

All records or any material about individuals must be kept secure and with the person's informed consent, Individuals must be informed that records will be kept on a Case Management System (Halo) in accordance with the Data Protection Act.

Where requests are made by individuals to see their files/records, the request should be referred to the line manager, who should check with EDAS's CEO regarding what information can and cannot be shared in accordance with the Data Protection Act 1998 (DPA) Policy.

In training, educational or media work, EDAS will not use any information that could identify a service user unless they have their express permission and the service user has signed a disclaimer form. Where a service user does agree to be named in any of this work, the risks to them doing so should be clearly outlined and the CEO of the service must be satisfied that this has happened.

All confidential information no longer required should be stored securely and then shredded in accordance with the Data Protection Act 1998 (DPA) Policy.

Confidential information should only be taken out of the office with the express permission of Line Managers. This information should be kept in a locked case and workers should ensure that any work they need to do outside of the office cannot be seen by anyone else and is locked away when not being worked on.

Workers should not access any files or documents to which they do not have appropriate authority to access.

Email Usage

Staff emails and passwords should not be shared unless there is a business reason for this to happen. Passwords should be changed regularly. Workers should be aware of appropriate use of secure e- mail e.g. Cisco, CJSM, Halo mail etc where e-mails are being sent/received to an outside service.

Recognised exceptions to this policy

Confidentiality policies are not intended to prevent the exchange of information between different professional staff when it has the purpose of:

- Ensuring the protection of children under the Children Act 1989, 2004.
- Ensuring the protection of vulnerable adults.
- Ensuring the protection of service users believed to be at risk of self-harm.
- Ensuring the safety and security of service users, staff or the wider community.
- Ensuring acceptable standards of professional practice.
- Monitoring and research where full name and address are not recorded.
- Ensuring the protection of the public, where there is evidence of risk of serious harm.
- The prevention, detection or prosecution of serious crime.
- Meeting requirements of the courts, coroners, some tribunals and persons appointed to hold enquiries have legal powers to require disclosure of confidential personal information. (NB. This can involve **all** clinical notes being subpoenaed).
- Giving information regarding a serious crime which has been committed, such as a murder, manslaughter, rape, treason or kidnapping (Police and Criminal Evidence Act 1984).
- Giving information about suspected terrorism (Prevention of Terrorism Act 1998).
- Meeting the requirements of the Mental Health Act 1983 where a service user objects to their 'nearest relative' being consulted re:-An application for Treatment Order (Section 3) is being considered
- An application for assessment and/or treatment in relation to the service user has been made
- Meeting the requirements of the Mental Health (Patients in the Community) Act 1995 where the service user is known to have propensity to violent and dangerous behaviour.

Breaches of Confidentiality

In an instance where an individual worker has been found to have inappropriately breached Confidentiality, the Team Leader/ Line Manager must address this and possible consequences should take into account the effects of a Breach of Confidentiality on both the Service, the organisation and the individual concerned. Depending upon the severity of the case, a breach of confidentiality could be classed as gross misconduct and lead to dismissal. The Halo custodian must also be notified of any breaches in confidentiality.

Appendix 1

ESSENTIAL DRUG & ALCOHOL SERVICES
Confidentiality Statement

I…… (Print name)

of……..
……
……
……

Understand that all information and work conducted by, and on behalf of the Essential Drug & Alcohol Services including the Trustees and Chief Executive, is totally confidential.

I therefore agree to abide by the EDAS Confidentiality Policy & Procedures at all times.

I understand that any disclosure of information of the service's work to persons outside of EDAS without consent will be considered a breach of confidentiality and may be classed as gross misconduct and may lead to dismissal.

Dated this …… Day of……20……

Signed……...Position…….

Witness…….Position……