OASIS Mental Health Support

Confidentiality Policy

Introduction

OASIS, as a user led and run organisation, are conscious of ensuring information is secure and used correctly. When it comes to data and information, the charity complies with employment law, (e.g. Data Protection Act 2018, UK GDPR, Public Disclosure Act 1996, Employment Rights Act 1996, Children's Act 2004, Rehabilitation of Offenders Act 1974, Prevention of Terrorism Act 2005.). This ensures that the organisation handles data correctly, and ensures that all user information, be it service user, staff, volunteer, donor, or other associated party, will have confidence in the ability of the organisation to ensure their information is being used correctly.

Based on these core beliefs, OASIS's Confidentiality Policy is necessary for the following reasons:

- To protect service users, employees, and volunteers from the possibility of information about them being passed on to individuals or organisations who have no right to that information.
- To reassure all parties that good care will be taken with information which they give to OASIS employees and volunteers and to enable them to trust those who are providing a service to them.
- To provide guidance to employees and volunteers on the extent to which confidentiality is to be preserved, circumstances in which they may breach confidentiality, and measures to be taken for the safeguarding of information.
- To assist OASIS employees and volunteers to comply with legal and statutory requirements for the disclosure of information.
- To reassure service users wishing to make a complaint to, or about, OASIS that the confidentiality of any complaint will be given high priority in so far as this is consistent with the need to investigate the complaint.

General confidentiality statement

- All OASIS employees and volunteers are required to respect the right of service users, other employees, and volunteers to privacy and confidentiality as far as possible within the constraints of legal requirements and the safety of other people.
- The fundamental principle of "need to know" should be an underlying consideration as to whether confidential information may be shared within the organisation.
- When information is given at the 'first point of contact', it is paramount that consent is obtained – eg during conversations by phone, in our open access Drop-in or Crisis services - it may be treated as information given to the organisation as a whole, and not confidential to that particular member of the organisation who that information is privy to.
- However, the sharing of any confidential information within OASIS should only routinely be allowed where it necessary for the delivery of services that the service user has requested - ie workers may share this with other colleagues involved in delivering those services requested.
- Information that has been collected will only be shared as per the consent form, amongst relevant members of the organisation and outside authorities, as and when required.

- Information will only be shared if it is relevant to the receiving party, e.g. there is a concern for the individual, linked parties, or express consent has been provided.
- Examples of where information given to one worker may be used to facilitate access for a person to use other services would be if, during the initial discussions, they disclosed they needed help with areas such as debt/benefits/counselling/preventing social isolation/help in accessing other community services etc; then, although we would usually seek specific permission, there would also be implied permission that we could pass on this request to the relevant specialist worker within OASIS. This would not, however, give us permission to discuss these needs with any other agency without express permission. The consent of the person, whose information is to be passed on, will be sought, and they will be informed what information has been passed on and to whom it has been passed.
- Other areas where Confidential information may be shared **within** the organisation are:
  a) staff working with the same person sharing awareness of an issue of concern around an individual – this will usually be within the daily Drop-in/Crisis services - to facilitate continuity of approach/support to a person or for issues regarding staff wellbeing (eg handling service user crushes or people monopolising the time of one particular worker etc).
  b) for the purpose of advice/guidance or personal support during/following a difficult or distressing phone call/in-person incident. In most cases it will not be necessary for the person providing that support– usually the CEO but it may be other colleagues or the OASIS Chair - to know the details of the individual involved, just the requests being made/scenario/issues of concern etc in order to give guidance, advice and support, thus maintaining confidentiality. On some occasions, however, these details will be known – either by the need for direct disclosure (eg if there are possible threats to a third party/issues that relate to Safeguarding etc) or by the CEO having an awareness of an on-going situation. In these circumstances staff will still aim to share only the relevant 'need to know' information relating to the issues being discussed.

- Confidentiality will not be breached outside of the organisation (ie given without either being requested to do so by the person, or permission being sought and granted) in the 'best interests' of the service user; except in the particular circumstances detailed within this Confidentiality Policy and will follow a Risk Assessment protocol.
- This policy covers not only information given deliberately by the person concerned, or – with permission - by other people/agencies regarding the person; but also, information acquired accidentally or through observation.
- All members of staff, volunteers and Trustees are expected to familiarise themselves with this policy and to ensure that they respect and uphold its provisions. Appropriate disciplinary action will be taken against anyone who disregards the policy.

Circumstances in which confidentiality may be breached

1. **Legal and statutory requirements**

The general law does not give an absolute right to confidentiality except where there is a contractual provision to this effect.

Legal and statutory requirements affecting OASIS include, but are not limited to:

- Reporting of safeguarding issues if the service user is believed to be the subject of a safeguarding risk.

- Reporting of safeguarding issues if there is belief someone is a threat to a child or vulnerable person.
- Obligation to report under RIDDOR
- Reporting notifiable diseases to the Chief Executive of Public Health where appropriate.
- Reporting accidents at work to the Health and Safety Executive under RIDDOR.
- Replying to certain specific enquiries from Government Departments e.g. DWP, or the Inland Revenue. Not all such enquiries are covered by statutory requirements so a check on the legal status of the request should be made before supplying information.
- Passing on information to the police on terrorist activities and information requested on road accidents involving personal injury.
- Giving evidence in court if a subpoena is issued.
- Providing information to the police in the case of suspected or actual terrorism.

Legislation that may apply in the above situations and to our work generally includes: Care Act 2014, Children and Social Work Act 2017, Working Together to Safeguard Children 2018, General Data Protection Act (GDPR) 2018, Data Protection Act 2018, RIDDOR 2013, the Human Rights Act 1998, the Crime and Disorder Act 2008, the Mental Capacity Act 2005, employment law, Public Disclosure Act 1996, Employment Rights Act 1996, Children's Act 2004, Rehabilitation of Offenders Act 1974, Prevention of Terrorism Act 2005.).

2. Duty of care

OASIS owes a duty of care to the users of its services, staff and volunteers. It may therefore be necessary to breach confidentiality where a service user is acting, or likely to act, in a way that could cause serious physical or emotional risk to themselves or others.

OASIS also owes a more general duty of care towards members of the public. It may be necessary to pass on information to the police or statutory authorities where there is considered to be a serious risk to a particular person or persons, or to the public in general.

This duty of care should be considered in conjunction with section 3.

OASIS employees and volunteers share with all citizens a duty of care towards children and vulnerable adults. If OASIS employees know or suspect that a child or vulnerable adult has been, or is currently at serious risk of being, abused/harmed, the procedure set out in OASIS's Safeguarding Children or Safeguarding Adults Policies should be adhered to.

3 Passing on information to others

Where there is no legal obligation, but there may be a duty of care to pass on information, the decision whether or not any action should be taken will be discussed by the staff on duty using the following protocol, being:

If a service user poses an immediate risk of harm to themselves, members of staff, volunteers, or the public, then the Emergency Services (999) <u>MUST</u> be called immediately.

Ensure that the current location of the service user is provided. If this information is not available, provide them with the contact details of the service user and any known addresses if possible.

Non-Emergency Risks to be assessed by the staff of the organisation and is for service users who have not expressed any immediate harm, danger, risk to themselves or others. If a breach of confidentiality is required:

- Explain to the service user the reasons why their information is being shared and who to.
- If appropriate, contact the relevant services (GP, Emergency Services, CAMHS, SOLAR, etc.) whereby there is no immediate harm or danger, but additional support may be required.
- Create an action plan with the service user on the steps being taken, bespoke to them, to ensure they are supported throughout the process.

Determination of Risk

Immediate risk includes:

- The service user has expressed that they are suicidal, expressing suicidal ideations, self-harming, threatening members of staff or general public, violence towards members of staff or general public.
- Possession of any weapons, drugs or alcohol, regardless of use, intent or consumption.
- A raised concern/alert from a non-service user due to intentions or actions (e.g. a threat has been discussed with someone outside of the organisation).

Keeping Information Secure

OASIS employees and volunteers must:

- Not be overheard when discussing confidential information on the phone, or with the service user or appropriate staff.
- Not leave information held in paper format where it can be potentially seen by others, and to keep such confidential information in locked filing cabinets when not in use.
- To keep records which include no more than the minimum information required.
- To destroy information (paper or electronic), when it is no longer required, in accordance with the guidance notes for implementing our data protection/GDPR policy.
- Any service user information stored on the OASIS QPOP system, will be password protected.

Complaints

People who wish to make a complaint either about any aspect of OASIS's services or about a OASIS employee, volunteer, or Trustee/Director, may be concerned about the confidentiality of information they are giving. The preservation of confidentiality will be given high priority, subject to the previous exceptions listed. Sometimes, if the complaint is to be thoroughly investigated and action taken because of the complaint, it may not be possible to avoid a breach of confidentiality. The permission of the complainant will always be sought for this but in cases where the welfare of the complainant or other people is seriously at risk it may be necessary to breach confidentiality even if that permission is withheld.

Access to information

Service users, employees and volunteers have a right to see any personal information kept about them by OASIS; this procedure is covered in OASIS's Policy on GDPR and Data Protection.

Further notes on the implementation of this policy

- OASIS's policy on confidentiality will form part of terms and conditions of employment of paid and unpaid staff.
- OASIS's policy on confidentiality will apply to Trustees/Directors, employees, and volunteers. Breaches of the policy will result in disciplinary action.
- Training will be provided to Trustees/Directors, employees and volunteers regarding the nature and implications of the policy.

This policy should be read in conjunction with other relevant policies e.g. Complaints Policy, Adult or Child Safeguarding Policy, Data Protection Policy, Guidance notes on data collection and retention HR policies, volunteering, trustee recruitment, DBS, Social media, home working, and all other appropriate and applicable policies.

Next review date: April 2025