Allsorts Limited Confidentiality policy and guidance

1. Introduction

Every person has the right to expect that information held about them will be handled sensitively. By producing a policy on confidentiality, Allsorts is underlining its commitment to that right and aiming to set high and consistent service standards.

During the course of their duties, staff and volunteers may be given information of a sensitive nature; for example, details about an individual's health or financial situation. It is important that staff and volunteers understand and accept their responsibility not to pass on this type of personal information. It is also important that staff and volunteers are familiar with the support network open to them within the organisation should they need to discuss any information they have been given. e.g. with their manager.

Allsorts is required to comply with legislation. This policy has been developed taking into consideration legal obligations including the Data Protection Act 1998 and Human Rights Act 1998

The Data Protection Act

The Data Protection Act places a number of requirements in the manner in which data concerning individuals is stored, handled and shared with other parties. The act distinguishes between personal data, any data pertaining to an individual and sensitive personal data. Sensitive personal data is any data that relates to:

- Racial or ethnic origin
- Political opinion
- Religious belief
- Union membership
- Physical or mental health
- Sexual life
- Criminal offences

Sensitive data can only be shared with the explicit consent of the data subject.

Allsorts has a Data Protection Policy

2. Definition of confidentiality

The definition of confidentiality used here means the protection of the rights of individuals to control information held or disclosed about them by Allsorts.

The individual

Individuals place a high level of trust in Allsorts volunteers and staff when disclosing information about themselves. An individual should be able to assume any information they give will only be used in connection with the reason they gave it. They should feel confident that it would not be used for other purposes or given to a third party without their consent. This only changes if certain legal bodies, for example the courts, request information.

The organisation

Staff and volunteers are entrusted with information, which is confidential to the organisation, rather than the individual volunteer or staff member; for example, financial information or plans to bid for external contracts.

Staff and volunteers must seek written permission before disclosing or publicising any such information concerning Allsorts generally, or their services therein.

Limited confidentiality means Allsorts staff will breach confidentiality: -

- If a service user poses a risk to themselves or others
- If a service user discloses an intention to commit an offence of any kind
- If there was a disclosure of abuse or threats of abuse

3. The practical applications

Any information received should be treated and shared on a strictly need to know basis.

This information remains confidential after the volunteer or staff member has stopped volunteering or working for Allsorts.

Confidentiality applies whether the receiver of information is told formally or informally.
Need to know

Information should only be shared within the organisation or with partner organisations on a strictly need to know basis. Need to know means information volunteers and staff need to help them work effectively.

Examples:

- *Sharing details on a specific piece of work referred to Allsorts - like Short Breaks as part of a wider care package.*
- *Allsorts could pass on contact details to local agencies on behalf of an individual moving to a new area but only with the permission of the individual.*

Passing on information

Information should only be passed on to people outside Allsorts with the express consent of the individual concerned. This should be written consent if the information is about sensitive issues like a medical condition. Verbal consent recorded in case notes may be appropriate in some cases.

It should be stressed that consent should be informed consent, i.e. the reasons for sharing/not sharing information, should all be discussed with an individual. All

Refusing consent

Individuals have the right to refuse consent to information being passed on to third parties except:

- Where there are reasonable grounds to believe the individual is at risk
  Example: A young person attending a short break tells a volunteer they have taken an illegal substance. They subsequently become unconscious and are taken to hospital. Information about the illegal substance could be critical to the treatment administered.

- Where there are reasonable grounds to believe the individual has, or will put someone else at risk.

- Where Allsorts is legally compelled to give information to statutory authorities or those legally authorised to request it like the courts, or under the prevention of terrorism act or where there is a statutory obligation (e.g. to the serious fraud office). Before any information is handed over in these circumstances legal advice should be taken.
  Example: An Allsorts staff member receives a witness summons to give evidence in court about a service user's affairs.

Decision making

Any decision to disclose information should be taken by the manager in consultation with the volunteers and staff involved and ideally after seeking guidance from the trustees.

Breach of confidentiality

Breaches in confidentiality may jeopardise the well being of staff and members. When working with vulnerable people it is essential to create a trusting relationship. However,

vulnerable people should think very carefully before making certain types of disclosures and be aware that a limited confidentiality policy is operational

Any intentional or accidental breach of confidentiality should be treated with the utmost seriousness and investigated as a matter of urgency under the disciplinary procedures. Any personnel who breach confidentiality may be liable to disciplinary action.

- Confidentiality is inappropriately broken
- Inappropriate use of data held by Allsorts
- Disclosure of client or staff details to unauthorised parties

Limited confidentiality means Allsorts staff will breach confidentiality: -

- If a service user poses a risk to themselves or others
- If a service user discloses an intention to commit an offence of any kind
- If there was a disclosure of abuse or threats of abuse

In these instances Allsorts may give information to statutory/emergency services.

4. Good practice

Maintaining and developing an effective confidentiality policy depends on delivering a consistent approach. This gives service users and other agencies trust and confidence in Allsorts. For the policy to work, all volunteers and staff need to be clear what procedures to follow and what information sources are open to them.

The following good practice guidelines will assist staff in the practical application of this policy.

Written information about service users should be factual, and avoid opinion and personal comments from volunteers and staff.

- If a volunteer or staff member has concerns about information they have received they should discuss this with their manager in the first instance.
- Volunteers and staff need to know they are free to discuss anything regarding service users with their line manager should they need to.
- A private space should be provided where possible for people to use when discussing services they may want to use or for discussing ongoing work.
- A private space should be used to discuss any issues of a personal or sensitive nature.

If a worker receives a contentious or difficult unsolicited disclosure and is asked to keep it to themselves, they will need to make clear that staff may need to share information with their Line Manager and that it is possible for staff to:

- Refuse to agree to a contract of absolute confidentiality and
- Not to continue a conversation if they feel that it may be heading in an area of disclosure they are not happy to take on board. Wherever possible, consent is sought to share this information.
- Information should never be given out over the phone unless:
- You are certain that you are aware of whom you are speaking to
- You return the call so that you are aware of whom you are speaking to

Members should never be discussed outside Allsorts service hours and only to authorised colleagues in connection with legitimate business.
The policy should be discussed with all staff and volunteers at induction. The implications of the policy for their work should be explained. Staff and volunteers must be fully supported at all times when dealing with issues of confidentiality, and individual support arranged for them if necessary.

The learning and development needs of volunteers and staff dealing with issues of confidentiality need to be identified and addressed. Staff and volunteers need to feel comfortable in asking for information needed to carry out their work and in keeping that information confidential.

5. Information storage

Good record keeping is essential to the smooth running of services and to keep standards consistent. To ensure systems used offer an acceptable level of security for information, the following guidelines should be observed.

- Job application forms, job interview records and job monitoring forms are confidential to Allsorts. The interview panel will hand in all papers at the end of interviews.
- References: When references for new employees are requested, it will be made clear that the references will be available only to the staff member concerned, otherwise they will be confined to the Personnel Sub-Committee.
- Supervision: with the exception of disciplinary action, information discussed in supervision will be confidential to the people concerned in the meeting and the Personnel Sub-Committee.
- All information about individuals should be recorded according to the agreed procedures, using standard forms that incorporate information on data protection.

- All records, electronic and manual, should be processed and stored securely. For example: using lockable cabinets to store paper information and using password protected files on software.
- If files are opened and moved from their secure storage, e.g. details printed from a computer or a paper file taken from the office, the volunteers and staff using them are responsible for maintaining the privacy of the information contained in those files and for ensuring the information is returned or stored securely as soon as possible.
- Access to files should be limited to those who need the information to carry out their work.
- Information should not be left out on desks in areas where the public have access.
- Records and any other written material should be kept for the recommended length of time. This means large amounts of information may need to be stored. Secure archive facilities need to be considered.

These guidelines cover all forms of information including telephone, email, fax (incoming and outgoing), post and electronically and manually stored records.