CLAPA Data Protection and Confidentiality Policy

1 Purpose

1.1 The purpose of this policy is to outline how the Cleft Lip and Palate Association (CLAPA) will manage personal information to ensure the confidentiality of our stakeholders is respected.

This Policy sets out CLAPA's systems regarding data collection, the maintenance of confidentiality, and the sharing and management of records. We are committed to protecting and safeguarding our staff and volunteers and also wider members of the CLAPA Community, with whom we come into contact.

2 Scope

2.1 This Policy is a guide for all staff and volunteers with regards to confidentiality and information sharing, particularly, but not exclusively, in relation to the cleft population. It is intended to help CLAPA staff and volunteers to understand, in what situations, information may be shared and with whom. The policy applies to all employees, volunteers and any other representatives of CLAPA who have access to personal information. For the purpose of this policy, employees and volunteers are referred to as 'staff'.

This policy applies to the confidentiality of all employees, volunteers, potential employees and volunteers, ex-employees and volunteers, secondees and trainees, service users, customers, donors, consultants, contractors and any other individual or organisation that has contact with the organisation directly or indirectly.

3 Rationale

3.1 This policy is necessary for CLAPA to fulfil its legal obligations, legal frameworks and to operate under best practice, which is set out in the:

- Data Protection Act 1998
- Human Rights Act 1998 (Article 8)
- Children Act 2004
- Mental Health Act
- Department of Health Policy of Confidentiality

4 Policy Statement

4.1 CLAPA will respect and maintain the confidentiality of all personal information in its possession and ensure personal information is only used for the purposes for which it was given. Staff will ensure that the sharing of information with third parties only takes place with the full and informed consent of all those involved. If consent is not given, information will only be shared to comply with legal obligations and CLAPA's duty of care.

CLAPA recognises the right of individuals who use the Charity's services to confidentiality and that they have a right to expect that personal details will be kept confidentially and in line with the requirements of law.

5 Responsibilities

5.1 The Chief Executive has a statutory duty to ensure the organisation complies with all legal requirements. The Chief Executive is ultimately responsible for the confidentiality of personal information across the organisation and has responsibility to ensure that the organisation complies with information governance requirements, including confidentiality and data protection.

The Chief Executive is responsible for ensuring effective systems are in place to avoid breaches of confidentiality with regard to personal information.

5.2 Owners of information are responsible for ensuring records are:

- held with informed consent;
- only relevant for purpose held; and
- kept accurate and up to date.

5.3 All CLAPA staff are responsible for:

- ensuring that personal information is kept secure and confidential at all times, including those occasions when it is necessary to remove it from the site, or for those staff who work from home;
- ensuring that relevant passwords are confidential; and
- reporting any incident that could possibly relate to a breach of confidentiality, e.g. loss, theft, corruption of information, password misuse, to the designated Data Protection Officer.

An individual's approach is treated as being to the organisation, rather than the individual worker. As such discussion of issues relating to individuals within the organisation, on a 'need to know' basis, are permitted under this policy.

6 Privacy

6.1 Staff must always be conscious of their responsibility to protect the privacy of people who use CLAPA's services. Personal information should not be discussed by staff in places where they may be overheard. Personal information should only be discussed in relation to the provision of support. All staff and people using CLAPA's services must be made aware that the information they give may be recorded, and shared, and for which purposes. Staff must be able to explain the implications of disclosing or not disclosing information to ensure people can make informed choices.

6.2 Staff must ensure that personal information about people who use services is stored securely and that access is restricted as far as possible. A clear desk policy must be adopted.

Confidential or personal information must never be left unattended, or where it might easily be accessed by a third party who is unauthorised to have access. This includes:

- Leaving information in an unlocked or empty office;
- Leaving information on the screen of an unattended PC;
- Allowing another person access to personal passwords inappropriately; or
- Positioning a PC screen so that it is visible to others.

6.3 The fact that an individual has made contact with the organisation will not be divulged without their consent. This includes ensuring messages are not left on answerphones or with 3rd parties that could indicate this.

6.4 Confidential or personal information must be disposed of when it is no longer required.

6.5 Any form of information that could adversely affect CLAPA's reputation should be considered as confidential and not be used or disclosed to third parties unless required by exception.

7 Sharing Information

7.1 Staff must seek the permission of people using CLAPA's services to share personal information.

Staff must explain to the person the following:

- Who the proposed information will be shared with
- What information will be shared
- The amount and detail of the information that will be disclosed
- The circumstances around which information may have to be disclosed without consent

Staff must seek consent from people using CLAPA's services should their information be required for purposes other than direct support, or other than for the purpose for which it has originally obtained.

8 Sharing information about children and young people

8.1 A young person aged 16 or 17, or a child under 16, who has the capacity to understand and make their own decisions, may give (or refuse) consent to sharing. Children, aged 12 or over, may also have sufficient understanding. When assessing a child's understanding, staff should explain the issues to the child in a way that is suitable for their age, language and communication development.

The following criteria should be considered in assessing whether a particular child, on a particular occasion has sufficient understanding to consent, or refuse consent, to sharing information about them:

- Can the child understand the question being asked of them?
- What are the implications of sharing that information, and of not sharing it?
- Does the child have a reasonable understanding of:
    - what information might be shared?
    - the main reason or reasons for sharing the information?
    - the implications of sharing that information, and of not sharing it?
- Can the child or young person:
    - appreciate and consider the alternative courses of action open to them?
    - weigh up one aspect of the situation against another?
    - express a clear personal view on the matter, as distinct from repeating what someone else thinks they should do?

8. 2 In most cases, where a child cannot consent or where it is judged they are not competent to consent, a person with parental responsibility should be asked to consent on behalf of the child.

Where parental consent is required, the consent of one such person is sufficient. In situations where family members are in conflict, staff should consider carefully whose consent should be sought. If a child or young person is competent to give consent, their consent or refusal to consent is the one to consider even if a parent or carer disagrees.

9 Refusal by an individual to authorise the sharing of information

9.1 Staff and people using CLAPA's services have the right to object to the use and disclosure of confidential or personal information and need to be made aware of this right. Where the person refuses to give permission to disclose personal information, staff will record this on their personal record.

9.2 If CLAPA has a duty to share the information, the person will be given a clear explanation of why the information has to be disclosed against their wishes. This will be documented.

10 Circumstances where information must be shared

10.1 There are a number of situations and circumstances where it is necessary to share information with relevant people. The following list, although not exhaustive, provides a number of instances where information must be shared:

- Where it is necessary to disclose information without consent in order to fulfil CLAPA's duty of care to the person or because there is an overriding public interest.
- In supervision or a team meeting related to a person where the wellbeing of the person using the service and/or CLAPA's duty of care is being reviewed. This includes disciplinary investigations about CLAPA staff.
- Where there is concern that a child or adult is at risk of harm. Normally this decision will be taken in consultation the Designated Safeguarding Officer (DSO) or the line manager. Where it is not possible to contact a manager, and there may be an immediate risk of harm, staff should contact Social Services, without the direction of a manager (see Child Protection Policy and Vulnerable Adult Policy).
- Where there is concern that a third party is at risk from harm by the actions of another person.
- Where there is a concern that a person may carry out serious self-harm.
- Where a Court of Law has instructed a representative of the Charity to divulge information, for example the police can apply to a judge for an order under the Police and Criminal Evidence Act 1984 (PACE).
- Where there is a concern the person may commit a serious criminal offence.
- If there is a reason to believe the individual is withholding consent but does not have mental capacity to make an informed decision
- The need to share information is urgent and the person cannot be contacted. Unless there are exceptional circumstances, the person must be informed at the earliest opportunity of the disclosure.
- Seeking consent could interfere with a criminal investigation.
- Seeking consent could put the member of staff or third party in danger.

10.2 The decision about whether or not to share information and the reasons need to be recorded on the person's personal record on CLAPA's secure database. If the decision is to share, record what information was shared and with whom. If the decision is not to share, the reasoning for this needs to be recorded.

Advice will need to be sought from social services if the person may not have the capacity to give informed consent.

Staff must seek advice from the Chief Executive regarding any requests for information from the Police.

11 Assessing whether to breach confidentiality without consent

11.1 Staff are responsible for any decision they take to breach the confidentiality of an individual and disclose information to an agency or individual outside of the organisation. They must be able to evidence, through good record keeping, that they are able to justify their decision. Where possible, they should consult with their line manager or the Chief Executive.

When assessing whether the confidentiality of a person needs to be breached without their consent, the starting point should be the person's right to privacy under the Human Rights Act 1998. In order to disclose there needs to be an overriding public interest to disclose the information, for example, where there is a need to protect the health of others or the prevention of a serious crime.

12 Type and level of information that can be disclosed

12.1 In general, disclosures of confidential or personal information should only be made in accordance with the Data Protection Act and if the person making the disclosure is authorised to do so as part of their job.

Information should only be disclosed to people who need to know it and kept to a minimum. The information should be relevant, honest, factual and only sufficient to ensure that CLAPA's duty of care is fulfilled. The information disclosed should be proportionate to the issue being dealt with.

Even when consent has been obtained, confidential or personal information must still only be used in ways that safeguard the confidentiality of that information, including appropriate anonymity whenever and wherever possible.

When there is doubt over the detail or degree of information to disclose, clarification sought from the line manager or the Chief Executive. Requests for information from the media must always be referred to the Communications Officer, as per the Communications Policy.

12.2 Staff are in a position of trust and must never abuse that trust by passing confidential or personal information to family, friends or carers or by using such information for personal or commercial gain.

13 Data protection

13.1 It is necessary for CLAPA to collect personal data and other information about an individual in order for it to carry out its functions as a service provider, fundraising organisation, employer and provider of volunteering opportunities.

We will as far as reasonably possible takes steps to ensure the information collected is accurate and relevant to the purpose it is being collected for. At the point of data collection an individual will be informed as to the purpose and what the data will be used for, and their permission will be recorded.

13.2 Principles:
Personal data will be used for the purpose for which it was given.
Personal data will be collected and processed fairly and lawfully.
Data collected will be adequate, relevant and not excessive in relation to the purpose collected for.
As far as practicable, steps will be taken to ensure that data is accurate and, where necessary, up to date.
Individuals will have a right of access to any records which relate to them personally, including any information from other parties.
Data shall not be kept for longer than is necessary.
Technical and organisational measures will be taken against unauthorised or unlawful use of data.

14 Publicity

14.1 Where it is considered that information about a specific case would be useful for publicity or awareness raising purposes, the full consent of the individual concerned must be obtained and their identity fully protected unless they agree otherwise.

15 Compliance

15.1 The Chief Executive Officer has overall responsibility for the implementation of this policy.

Each individual is responsible for ensuring that they adhere to this policy at all times and for ensuring its correct implementation.

All staff members must be aware that there are possible disciplinary measures that can be taken for failure to comply with their responsibilities regarding the confidentiality and security of personal information, such as:

- Deliberately looking at records without authority;
- Discussion of personal details in inappropriate settings;
- Transferring personal information electronically without encrypting it.

Breaches of confidentiality or data loss may also result in criminal charges being brought against an individual staff member or CLAPA as an organisation.

15.2 The organisation recognises that it may, in some circumstances, have obligations under the Freedom of Information Act to disclose data or information and will comply with these, taking the requirements of the Data Protection Act into consideration.

15.3 The organisation also recognises an individual's right to request to see the information held about them. All such requests should be made in writing to the Chief Executive Officer. The organisation will make an initial response within 10 working days.

15.4 All staff are responsible for ensuring they understand the requirements of this policy, what it means to them in their role and for ensuring they abide by its requirements. They are also responsible for reporting any potential or actual breaches of this policy to their line manager.

16 Record retention and storage

16.1 The organisation will annually dispose of all relevant archived records in accordance with the Record Retention Standards. A confidential waste disposal service will be used to dispose of all records which include personal or other confidential data, both regularly throughout the year and annually. Each site also has a shredder for immediate destruction of information along with a confidential waste box and staff are trained in disposal of confidential material.

17 Related Documents

Child Protection Policy
Communications Policy