Confidentiality and the Appropriate Sharing of Information Policy

A. General principles:

It is the right of every person to their privacy and the right to expect that any personal information they pass on will be treated in the strictest confidence and not discussed with anyone else, or passed on to a third party; without their clear permission. The only exception to this is in circumstances where not to do so would place a child or vulnerable adult at risk of significant harm or where it is reasonable to suspect that a crime has been committed.

All the personal information held by Communityworks on children and adults, their carers, or other interested parties accessing our centre must always be respected. Breaches of confidentiality undermine both our duty of care to the people with whom we are working together and can bring our organisation into disrepute. It is therefore essential that every member of staff must respect the sensitive nature of personal information shared with us and take reasonable steps to ensure its integrity is maintained at all times.

Staff, volunteers, children and their parents/carers and other adults have the right to gain access to all information held about them, in accordance with Data Protection principles, and to correct any factual errors.

B. Rationale:

Everyone who works in or comes to Communityworks has a right to confidentiality. However, the term 'confidentiality' can be interpreted in different ways, so the purpose of this policy and the associated guidelines is to set out an agreed understanding of what confidentiality means within Communityworks.

We also must adhere to the requirements of the Data Protection Act 2018, Human Rights Act 1998, General Data Protection Regulations 2018 (GDPR) and other national and local protocols relating to the sharing of information.

Communityworks therefore has both a legal and ethical responsibility to protect the confidentiality of the information that it receives in the course of our work with children, adults and families.

C. Aims:

1. To ensure that in all decision making about information sharing, safeguarding and promoting the welfare of the child or vulnerable adult is the first consideration.
2. To ensure that there is an agreed understanding about the meaning and scope of confidentiality within Communityworks, and that it is a legal requirement.

3. To recognise people's right to privacy including staff, volunteers, children and families, and other adults and ensure that their confidentiality is respected.
4. To ensure that staff, volunteers and service users are clear about the different circumstances in which it may be necessary to share information with other agencies, particularly those circumstances in which this may be done without prior consent.
5. To ensure that Communityworks acts with transparency when making decisions about data including the processing, storage and deletion process and in responding to a Subject Access Request.
6. To ensure that personal information held by Communityworks is held securely and is not shared without the prior knowledge of the person concerned, unless to do so would put someone at risk or prejudice a police investigation into a serious offence or lead to an unjustifiable delay in protecting a child or vulnerable adult.

D. Objectives:

Our aims will be fulfilled through the following objectives:

a) We will provide clear guidance to staff, volunteers and Board of Directors within Communityworks about the circumstances in which information about staff, volunteers, children and families, and other adults can be shared within and outside the organisation. This will be done by the issuing of bespoke Privacy Notices.

b) We will support staff, volunteers and service users in ensuring that confidentiality is not breached and to enable them to challenge in situations where breaches may be happening.

c) We will only share information about children with other agencies with the consent of parents. The only exception to this is where a child would be placed at risk if the information was not shared.

d) We will make sure that every individual who shares their personal information with us understands why we collect it, what we do with it, who we share it with, where we store it, how long we keep it and their right to access it.

e) We will protect the confidentiality of staff employed at Communityworks by not disclosing any personal information to service users and ensuring that the personal information held by Communityworks is kept secure.

Guidelines for Confidentiality and the Appropriate Sharing of Information

E. Methods:

Communityworks hold two kinds of records on adults, children and their families attending the Centre.

1. Personal (Physical) Records
   a) These include signed consents, and correspondence concerning the child or family, reports or minutes of meetings from other agencies or staff concerning the child, an ongoing record of relevant contact with parents, and observations made by staff on any confidential matter involving the child such as developmental concerns or safeguarding issues.

   b) All confidential records are stored in a lockable cabinet and are kept secure by staff. Ultimate accountability lies with the CEO and the Board of Directors.

   c) Parents have access to the records in accordance with the GDPR in relation to records of their own child, but do not have access to information about any other child or family. Adults have the right of access to their own records.

   d) Attendance at all sessions is recorded on a paper register and these are stored in a locked filing cabinet.

   e) Staff will not discuss personal information given by parents with other staff members, except where it affects planning for the child's needs, or where there are concerns for the child's safety they should immediately raise their concern with one of our Safeguarding Named People. Staff should not engage in casual or social discussions about families.

   f) All members of staff sign to say they have read and understood this Policy.

2. Database records
   a) Adults and Parents/Carers of all children attending Communityworks complete a Registration form, at the bottom is an agreement that adults and parents sign to permit Communityworks to store information on the database. Attendance at all sessions is recorded on paper registers and this information is transferred onto the database. Attendance records are kept for Health and Safety Purposes. Each person completing a registration form is given a privacy notice. The privacy notice is also on our website and Google Translate can translate it into other languages.
   b) There are a number of staff and volunteer related databases; such as the Single Central Record which lists DBS records.

F. Other Records

1. Issues to do with the employment of staff, paid or voluntary, remain confidential to the people directly involved with making Personnel decisions.

2. Students on recognised qualifications and training are both DBS checked and advised of the Confidentiality policy and have to sign to agree to adhere to it.

3. Incidents are recorded on Incident Reporting Forms where there are concerns about the welfare of a child. These are kept in a locked filing cabinet.

4. Photographs and videos are only taken with the express permission of the adult or parent/carer. The nursery uses Early Essence to record children's progress and parents/carers have full access to all data held and are encouraged to contribute their own photographs and videos. Only those with a password are able to access the information about their child; however other nursery children may be in photographs and videos.

G. Operational Requirements

1. No personal information should be divulged to third parties without the permission of the person it is about, whether this be a user, friend, relative or carers, except in circumstances where we have a legal obligation to do so, or there is a serious threat to someone's health or safety. In such cases the Management Team should be consulted and / or legal advice sought before any information is released. In cases where there are conflicts of interest between parties it may be appropriate to open separate case files.

2. No information should be given without checking the identity of the person requesting it. If this is over the telephone or through other electronic means, the staff member must check first with the person making the request however persistent they may be. If there is any doubt about the person's identity or the reason for the request, information / details should not be divulged and the matter reported immediately to a Line Manager. Information sent by post should be properly addressed with an office stamp on the reverse of the envelope, so it can be returned unopened if undelivered. Personal data should not be sent by electronic means, unless its security can be guaranteed by the use of encryption.

3. Registration forms need to be up to date and must be completed again when the details change. The registration form has specific requests for consent that must be ticked to enable Communityworks to process certain data, such as personal files, photographs and to enable us to refer to third parties. Staff must ensure that these forms of consent are given as otherwise these types of data should not be used or processed. Registration forms are signed but do not require consent to be added to our databases (both electronic and paper).

4. Requests for access to case files and other personal records should be dealt with by making a written request to the CEO. Care should be taken to respond within the accepted time scales and only person specific information is provided, i.e. not about other people who may be interested in the case and who have given permission for it to be released. Line management advice should always be sought to confirm the correct procedures are being followed. In certain circumstances, a decision may be made not to release information. (For example if to do so might put another person at risk.) See Subject Access Request section I below.

5. Staff responsible for keeping case records should ensure that the information in it is relevant, and that fact and professional opinion are clearly identified. Information must never be recorded in a manner that is disrespectful or could be subject to legal challenge. Good practice supports user / carer involvement in the keeping of case records. Case files should be kept in accordance with policies and procedures.

6. Information which is not to be divulged because of its impact on the individual (e.g. in mental health cases), or it was given in confidence (e.g. in abuse situations or involving legal opinion) must always be clearly identified as such and retained in a separate section of the case record. Line management and / or legal advice must be sought in cases of doubt.

7. Case records or personal information should always be kept in the relevant workplace. On occasions when they are taken out of a workplace, they should be kept with the staff member and never left on open display, e.g. in vehicles. Particular care should be taken when speaking in public with colleagues, (e.g. on mobile phones) to ensure conversations are not overheard when personal details are being discussed.

8. The requirements of relevant legislation, e.g. GDPR, should be respected at all times.

9. All data subjects have been issued with a Privacy Notice, this includes people that access our services, staff and volunteers, Board of Directors and those with whom we share data, such as contractors. Those that fund Communityworks are required to produce Privacy Notices to Communityworks so that we can be confident that their processes are in line with our policies and procedures.

10. Councillors and Members of Parliament have no absolute right to personal information that should only be provided on a need to know basis. Requests for information from a Councillor or Member of Parliament should be directed to the CEO after initial details have been taken.

11. Students, casual agency or temporary staff must be reminded by the relevant supervisor and /or manager of their obligation to respect confidentiality. Any breaches of confidentiality must be reported to the relevant college, agency or personnel unit.

12. Respect of confidentiality must be referred to in each staff member's induction.

13. In situations where case records are jointly held with other agencies (e.g. health), particular care must be taken to ensure that their contents, storage and accessibility are respected and joint arrangements agreed about how they are managed. The same principle applies to the sharing of information in jointly worked cases. Service users/carers should usually be informed that this is likely to happen and their agreement to us doing that sought and if appropriate periodically reviewed.

14. Sources of information regarding a serious concern about a user or carer should be respected. Where this may not be possible (e.g. in certain legal situations), this should be made clear at the earliest opportunity, and line management and / or legal advice sought.

15. Staff must always be careful not to inadvertently divulge personal information about service users, carers or other people we are in touch with in a case in social situations (e.g. at the request of friends or neighbours).

16. All confidential paper documents should be disposed of by shredding, and documents awaiting shredding kept in sealed bags (locked away if unattended). Computer held data should be deleted in line with policies and procedures. All data should be held in line with our Data Retention Policy and Data Audit Register.

17. In administering, filing, printing, typing or faxing confidential information you should ensure that it is undertaken by a person who understands the confidentiality procedures. It is

essential that confidential material is not left in machines after processing.

18. Care should be taken when passing on confidential information electronically by e-mail or Fax. In the case of Faxes, contact should be made with the recipient to ensure that they are aware that the information is being sent and can confirm when it has arrived. In the case of e-mails, confidential information should only be sent using a secure email system (Protonmail or Galaxkey) or by the use of a password protected attachment; a disclaimer should be added to the bottom of e-mails to the effect that the information contained in it is for the attention of the named recipient only and the sender should be notified if someone else has received it in error. The password should be communicated by telephone.

19. Computer passwords must not be easily identified. Users should keep these confidential. Personal computers should not be left unattended whilst the user is logged on. A screensaver, protected by a password, must be invoked when a PC has not been used for 10 minutes or more.

20. It is expressly forbidden to divulge any confidential information about Communityworks or anyone that has a connection with the organisation on social networking sites such as Facebook and others, private emails and Twitter.

21. Pictures will only be used for publicity with the express permission of all the people in the picture; this includes our newsletter and social media postings. Pictures will not be tagged.

22. Supervision sessions, meetings, courses and conversations should observe the same standards as written information, making levels of confidentiality clear or seeking clarity, if you are not told of the confidentiality level. On training courses this should be explicit from the outset.

23. You shall not remove from the place of your employment any documentation of any description nor take copies of such documentation for your personal use or the use of a third party either during your employment or on termination of your employment.

24. The main data risks are outlined in our Risk Register.

25. The CEO, in consultation with the Chair of Communityworks, is responsible for reporting any breaches to the ICO (Information Commissioner's Office) and Charity Commission. Communityworks is registered with the ICO. The Board of Directors will monitor our obligations as outlined within this policy and the law.

26. Concerns or complaints from a service user, their carer or other interested party should be relayed to the CEO, unless the complaint is about the CEO in which case it should be referred to the Chair of the Board of Directors.

H. Confidentiality regarding Staff Health

1. Managers need to know how long and why a member of staff is absent, they do not need specific medical details. However, where the absence will require changes to working arrangements more detailed information may be required. Employee's consent will be sought before this information is passed on.

2. Colleagues do not need to be informed of the reasons for a person's absence however they will need an indication of the absence period. Managers should remind staff of the confidentiality requirements if speculation or rumours begin.

3. All paperwork related to health issues is confidential. It must not be disclosed by staff with legitimate access unless authorised to do so, and must not be left open or unattended in files or on desks. All personal records should be locked away.

4. Employees' personal details should not be given to another employee unless this has been discussed and agreed previously.

I. Subject Access Requests

Data Subjects have a right to access information that Communityworks may hold on them. For staff this could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes. For people using our services this could include registers, case notes, CVs or referrals to a third party.

If an employee wants to see their personal data, they should speak to their line manager. Most requests for personal data can be provided quickly and easily.

If a member of the public wants to see their personal data they should make a Subject Access Request to the CEO. A subject access request should be in writing and include:

full name, address and contact details and details of the specific information required and any relevant dates.

Communityworks will respond within one month of the date of the request.

There will be no charge for Subject Access Requests, fees may only be required under GDPR if the requests are "manifestly unfounded or excessive".

If Communityworks refuses a request they must inform the individual within one month:

- why they have refused the request
- that the individual has the right to complain to the Information Commissioner's Office and to a judicial remedy. These details are outlined in the Privacy Notice.