Path: Confidentiality Policy

Policy statement
Path is committed to protecting people's privacy, ensuring that information about anyone is only shared with their express permission, other than where there are specific legal or protection requirements.

Legal basis
All staff members working at Path are bound by a legal duty of confidence to protect personal information that they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation in the UK: the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018).

Context
There are various factors which affect the information we ask of and hold about people, as well as how we use and share it. These include:

- Confidentiality, covered here
- Data Protection
- Legislation
- Partnership agreements
- Therefore, the agreements we have with people, themselves

Confidentiality
Within a service-providing organisation, confidentiality ensures any personal (as opposed to anonymous) information regarding clients or staff members or the organisation itself is only shared when strictly relevant, necessary and appropriate.

As indicated, it is important that members of staff also understand Data Protection, which addresses how and why we gather and store information. That is covered in separate policies and also relates to specific legislation.

Consent
Any and all clients supported by Path should be invited to sign a consent form, with an explanation of how information they provide may be stored, shared and used. That form will specific with whom information may be shared, as agreed with each client.

Sharing information
At Path, confidentiality operates under strict rules.
This means any information relating to:

1. the affairs of the agency, for example its plans or finances (not published on the Path website);

2. Path resources, such as information, reports, gathered material that Path has not otherwise published and which may be commercially sensitive;
3. clients who use the services of the agency;
4. staff of the agency;
5. visitors to the agency's premises;
6. information about other organisations that Path has a relationship with

is strictly confidential.

Therefore no information may be disclosed to anyone outside the agency, or relevant formal partnership* where relevant, without the person whom the information concerns freely giving their prior consent or without due reason (see below).

Particularly, therefore, information regarding anyone's:

housing status;
health status;
sexuality or sexual orientation;
name, address or telephone number;
political, religious or social affiliations;
employment or financial status;

may not be mentioned to anyone outside Path or relevant partners without the individual's free and prior consent.

* = Some services that Path is part of are multi-agency and so client confidentiality applies beyond Path. Any agreements with clients needs to reflect that.

Confidentiality Procedure

- Sharing information within the agency

Further, when information is passed within the agency it will be only to those for whom that information is necessary and relevant in terms of service provision or supervision.

i.e Workers may freely refer to client issues within line management relationships as part of being supervised and supported. They may also seek or provide advice from each other; but there will always be a reason for any such sharing and it should not compromise the client.

- Outside the Agency

When disclosing information externally to ensure there is no unreasonable invasion of privacy the following issues should be considered:

- Has the client / person given permission for disclosure to this party?
- Is the disclosure necessary and proportionate to the request? If the answer is no, then do not disclose the information.

- What is the receiving party intending to do with the information? If the purpose for which the information is being sought is for an unreasonable purpose then the information should not be disclosed.
- Does disclosure of this information affect Path commercially?

Consent forms for clients will cover who Path may give information to, such as the following:

- Family and friends of clients
- Police, courts and probation services
- Social workers and social services departments
- Researchers and educational institutions
- Funders / commissioners
- Other agencies as may be necessary eg other housing charities

No personal information about staff, volunteers or clients will be given to any third party including a member of their family, without the consent of the client, other than where relevant for public or individual protection. Information will only be divulged on a "need to know" basis.

Information will therefore only be passed to another agency or to other individuals outside of Path with the consent of the client. Where possible this will be with written consent. If a member of staff or volunteer intends to get information from another agency to help the client or to refer them to another agency then this must be explained to the client and their permission given.

The only exceptions to the above are when one or more of the following apply:

- There is overriding public interest to disclose the confidential information;
- Disclosure is necessary to:
    - protect minors;
    - prevent terrorism;
    - prevent life threatening situations (ie a risk of death or serious harm);
    - prevent a serious arrest-able offence or treason; or
    - detect, investigate and prevent a Serious Crime being committed.

Path is not obliged to disclose any information, unless ordered to do so by a court or a police warrant is obtained. However, it is our policy to co-operate with other authorities such as the Police, social services, the probation service, the courts and the NHS and to provide such authorities with confidential information relating to clients if one of the above criteria is present.

Before disclosing to the court or the police consideration should be given as to whether they have reasonable grounds to suspect that a serious crime may be committed and/or has been committed, unless there are statutory obligations to disclose the information. Information may also be disclosed to other third parties if required to do so by law (e.g. as in the case of the DVLA).

Examples of serious crimes may include but are not limited to:

- Abusing and/or assaulting third parties (including children);
- Drug trafficking;
- Murder;
- Rape;
- Assault;
- Fraud.

Disclosure of personal data

In the event that Confidential Information should be disclosed, Path will ensure that:

- the client's consent to disclose the information has been obtained and
- if no consent is obtained, ensure that the disclosure of the Confidential Information:
    - is anonymised in so far as is reasonable; and
    - keeps the disclosures to a minimum (i.e. only disclose information required for the purpose for which the information is sought; and
    - discloses the information only to the person who needs to know.

All decisions in relation to disclosure should be recorded in the client's case notes, so that an audit trail is available should a complaint be received from the client.

Specific Situations

These are the situations where Path might be required to pass on information to third parties and these are considered below. In each situation different considerations are required.

A. Clients themselves

This will be a "subject access request" - see "Subject Access" in Data Protection Policy.

In the event that Path discloses their personal data and/or confidential information to them, Path will not be in breach of their confidence as Path is simply complying with their request.

It is possible that a client may have given a Power of Attorney to another person to obtain such information from Path on his/her behalf. If such a person requests information under a Power of Attorney, workers should make sure

that they satisfy themselves that the person has the authority and are the person they say they are before disclosing any information to them.

In this case, workers should ask to see an original copy of the executed Power of Attorney and some form of identification (passport and/or driver's licence) before providing any information. If such documentation is provided, then disclose the information to them as if they were the client.

B. Employees of Path

There are two aspects to confidential information and employees: a) information about employees; and b) information about Path and how employees use it.

a) Routine record keeping and administration does not require consent. However, Path will only discuss or provide information in relation to a specific client to another member of staff if they "need to know".

   Also, workers should ensure that all information is secure so files must not be left open on desks or at home. Workers should ensure that all records are locked away and that a clear desk policy is maintained.

b) Many aspects of how employees may and may not use and share information are covered in this and Data Protection policies. In addition, employees need to understand and respect the fact that some of Path's information, forms, policies and more are resources developed and owned by Path which may be commercially sensitive. Some are available on Path's website and so are openly available; others may not therefore be shared with others without express and prior management consent.

C. Family and Friends

With family and friends, it is always recommended that consent is obtained from the client before disclosing confidential or personal data or that any explicit consent has not been withdrawn. However, if no consent can be obtained, disclosure may be justified if such disclosure is to close relatives such as a mother, father, children, wife, husband, partner and approved by a manager.

If they are friends, consent is required to disclose information about a client. If no consent is received information cannot be disclosed.

D. Police, courts and probation services

Confidential information may be shared with the police, courts and probation services, if it is for the purpose of detecting and/or preventing a serious crime. This should be pro-active and workers should not wait for the police to contact Path if workers suspect that the client might be involved in committing a serious crime.

In addition, if workers are contacted by the police, the courts and probation services asking Path to disclose confidential information in relation to the client, because they suspect that the client may be involved in or committing a serious crime, workers will be able to disclose such information without obtaining the client's consent.

Workers should ensure that a common sense approach is taken.

Social workers and social services departments
Before disclosing confidential information and/or personal data to Social Workers and Social Services Departments, consent should be obtained from the client to disclose information, if not already obtained.

However, if consent is not forthcoming, confidentiality and privacy can be breached if any of the exceptions listed above apply. For example, if there is reason to believe that a child is at risk from a wife, husband or partner.

Checklist
This checklist should be used when a request for information from a third party is received. However, if workers are in any doubt whether to disclose such information then the request should be discussed with the line manager.

1. What is the type of request?
2. Have you identified the person making the request for information? If it is the client it is a subject access request. If it is a third party consider, confidence and privacy.
3. Can the information be anonymised to achieve the same result?
4. Has the client signed the consent form?
5. Has the client revoked consent?
6. If there is no consent is the disclosure justified?
7. Ask a colleague for a second opinion as to justification.
8. Do you think that someone is fishing for information?

All decisions in relation to disclosure of confidential information and/or personal data should be recorded in the client's case notes, so that an audit trail is available should a complaint be received from the client.

Social media
Path has policies on Data Protection and Computer Use, which further cover use of personal information. One specific area is social media (covered in Computer Use): employees must adhere to confidentiality when using social media.

Telephone

If sharing personal information by phone, workers should ensure that the identity of the caller has been verified. Ask them a question that they should know before disclosing the information. If they do not provide the correct answer do not disclose the information.

Post and email

Workers should not send CDs or memory sticks with personal information through the post, unless it is password protected.
Equally, emails containing personal information should only be sent to and from secure email addresses.

Breaching this policy

Any breach of confidentiality will result in an investigation and/or that person(s) being disciplined. Serious breaches, especially if breaching service contracts or the law, may result in dismissal.

Relevant other policies:

- Computer Use;
- Data Protection.